



Proceedings

**DEXA**

# ARES 2006

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

20th-22nd April 2006

Vienna University of Technology, Austria

In Cooperation with



TECHNISCHE  
UNIVERSITÄT  
WIEN  
VIENNA  
UNIVERSITY OF  
TECHNOLOGY



OESTERREICHISCHE  
COMPUTER GESELLSCHAFT  
AUSTRIAN  
COMPUTER SOCIETY



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

IEEE Computer Society Order Number P2567  
Library of Congress Number Pending  
ISBN 0-7695-2567-9

ISBN 0-7695-2567-9



9 780769 525679

# **Proceedings**

The First International Conference on  
Availability, Reliability and Security

**ARES 2006**

---

Copyright © 2006 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved.

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

*The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.*

IEEE Computer Society Order Number P2567

ISBN 0-7695-2567-9

ISBN 978-0-7695-2567-9

Library of Congress Number 2006923025

*Additional copies may be ordered from:*

IEEE Computer Society  
Customer Service Center  
10662 Los Vaqueros Circle  
P.O. Box 3014  
Los Alamitos, CA 90720-1314  
Tel: +1 800 272 6657  
Fax: +1 714 821 4641  
<http://computer.org/cspress>  
[csbooks@computer.org](mailto:csbooks@computer.org)

IEEE Service Center  
445 Hoes Lane  
P.O. Box 1331  
Piscataway, NJ 08855-1331  
Tel: +1 732 981 0060  
Fax: +1 732 981 9667  
<http://shop.ieee.org/store/>  
[customer-service@ieee.org](mailto:customer-service@ieee.org)

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

 **IEEE**

IEEE Computer Society  
**Conference Publishing Services**  
<http://www.computer.org/proceedings/>

# Table of Contents: ARES 2006

## First International Conference on Availability, Reliability and Security

<b>Message from the Organizing Committee</b> .....	<b>xv</b>
<b>ARES and Workshops Committees</b> .....	<b>xvi</b>

### Invited Talks

Risk Management and Risk Assessment at ENISA: Issues and Challenges .....	2
<i>Louis Marinou</i>	
Model Driven Security .....	4
<i>David Basin</i>	

### Session 1: Trust Management

Trust Based Risk Management for Distributed System Security — A New Approach .....	6
<i>Ching Lin and Vijay Varadharajan</i>	
RATING: Rigorous Assessment of Trust in Identity Management .....	14
<i>Rajarajan Sampath and Deepak Goel</i>	
Provably Secure Anonymous Access Control for Heterogeneous Trusts .....	24
<i>Kilho Shin and Hiroshi Yasuda</i>	

### Session 2: P2P Systems

A Secure Event Agreement (SEA) Protocol for Peer-to-Peer Games .....	34
<i>Amy Corman, Scott Douglas, Peter Schachte, and Vanessa Teague</i>	
Satisfiability and Trustworthiness of Peers in Peer-to-Peer Overlay Networks .....	42
<i>Yoshio Nakajima, Kenichi Watanabe, Naohiro Hayashibara, Tomoya Enokido, Makoto Takizawa, and S. Misbah Deen</i>	
Tamper-resistant Replicated Peer-to-Peer Storage Using Hierarchical Signatures .....	50
<i>Alexander Zangerl</i>	
Censorship-Resistant and Anonymous P2P Filesharing .....	58
<i>Regine Endersleit and Thilo Mie</i>	

### Session 3: Mobile Network and Pervasive Systems

A Dependable Device Discovery Approach for Pervasive Computing Middleware .....	66
<i>Sheikh Ahamed, Mohammad Zulkernine, and Suresh Anamanamuri</i>	
Single Sign-On Framework for AAA Operations within Commercial Mobile Networks .....	74
<i>Saber Zrelli and Yoichi Shinoda</i>	
A Selector Method for Providing Mobile Location Estimation Services within a Radio Cellular Network .....	82
<i>Junyang Zhou and Joseph Kee-Yin Ng</i>	

Guidelines for Biometric Recognition in Wireless System for Payment Confirmation _____	90
<i>Leon Grabensek and Sasa Divjak</i>	

#### **Session 4: Protocol and Communication**

An Extended Verifiable Secret Redistribution Protocol for Archival Systems _____	100
<i>V.H. Gupta and K. Gopinath</i>	

Analysis of Current VPN Technologies _____	108
<i>Thomas Berger</i>	

Integration of Quantum Cryptography in 802.11 Networks _____	116
<i>Thi Mai Trang Nguyen, Mohamed Ali Sfaxi, and Solange Ghernaoui-Hélie</i>	

Availability Constraints for Avionic Data Buses _____	124
<i>Alban Gabillon and Laurent Gallon</i>	

#### **Session 5: Security as Quality of Service**

Securing DNS Services through System Self Cleansing and Hardware Enhancements _____	132
<i>Yih Huang, David Arsenaault, and Arun Sood</i>	

Personalized Security for E-Services _____	140
<i>George Yee</i>	

Providing Security Services in a Multiprotocol Service Discovery System for Ubiquitous Networks _____	148
<i>Juan Vera del Campo, Josep Pegueroles, and Miguel Soriano</i>	

Towards a Stochastic Model for Integrated Security and Dependability Evaluation _____	156
<i>Karin Sallhammar, Bjarne Helvik, and Svein Knapskog</i>	

#### **Session 6: Networking and Fault Tolerance**

A Novel Artificial-Immune-Based Approach for System-Level Fault Diagnosis _____	166
<i>Mourad Elhadef, Shantanu Das, and Amiya Nayak</i>	

Sandboxing in myKlaim _____	174
<i>René Rydhof Hansen, Christian W. Probst, and Flemming Nielson</i>	

Evaluation of Network Robustness for Given Defense Resource Allocation Strategies _____	182
<i>C.-H. Chen, Y.-L. Lin, Y.-S. Lin, P.-H. Tsang, and C.-L. Tseng</i>	

Proxy Oblivious Transfer Protocol _____	190
<i>Yao Gang and Feng Dengguo</i>	

#### **Session 7: Identification and Authentication**

Providing Response Identity and Authentication in IP Telephony _____	198
<i>Feng Cao and Cullen Jennings</i>	

Towards a Framework of Authentication and Authorization Patterns for Ensuring Availability in Service Composition _____	206
<i>Judith E.Y. Rossebø and Rolv Bræk</i>	

An Optimal Round Two-Party Password-Authenticated Key Agreement Protocol \_\_\_\_\_ 216  
*Maurizio Adriano Strangio*

A Method for the Identification of Inaccuracies in Pupil Segmentation \_\_\_\_\_ 224  
*Hugo Proença and Luís Alexandre*

Availability Enforcement by Obligations and Aspects Identification \_\_\_\_\_ 229  
*Frédéric Cuppens, Nora Cuppens-Bouahia, and Tony Ramard*

### **Session 8: High Availability and Dependability**

An Integral IT Continuity Framework for Undisrupted Business Operations \_\_\_\_\_ 240  
*R.W. Helms, S. van Oorschot, J. Herweijer, and M. Plas*

Highly Adaptable Dynamic Quorum Schemes for Managing Replicated Data \_\_\_\_\_ 245  
*Oliver Theel and Christian Storm*

High Availability Support for the Design of Stateful Networking Equipments \_\_\_\_\_ 254  
*Pablo Neira Ayuso, Laurent Lefevre, and Rafael M. Gasca*

A Hybrid Network Intrusion Detection Technique Using Random Forests \_\_\_\_\_ 262  
*Jiong Zhang and Mohammad Zulkernine*

Identifying Intrusions in Computer Networks with Principal Component Analysis \_\_\_\_\_ 270  
*Wei Wang and Roberto Battiti*

### **Session 9: Reliability and Availability**

Systematic Error Detection for RFID Reliability \_\_\_\_\_ 280  
*Sozo Inoue, Daisuke Hagiwara, and Hiroto Yasuura*

Feasibility of Multi-Protocol Attacks \_\_\_\_\_ 287  
*Cas Cremers*

Diversity to Enhance Autonomic Computing Self-Protection \_\_\_\_\_ 295  
*Michael Jarrett and Rudolph Seviara*

Reliability Forecasting in Complex Hardware/Software Systems \_\_\_\_\_ 300  
*Javier Cano and David Rios*

Availability Modeling and Analysis on High Performance Cluster Computing Systems \_\_\_\_\_ 305  
*Hertong Song, Chokchai "Box" Leangsuksun Raja Nassar, Narasimha Raju Gottumukkala, and Stephen Scott*

### **Session 10: Security and Privacy Issue**

Schedulability Driven Security Optimization in Real-time Systems \_\_\_\_\_ 314  
*Man Lin and Laurence Yang*

Ensuring Privacy for E-Health Services \_\_\_\_\_ 321  
*George Yee, Larry Korba, and Ronggong Song*

The Security Issue of Federated Data Warehouses in the Area of Evidence-Based Medicine \_\_\_\_\_ 329  
*Nevena Stolba, Marko Banek, and A Min Tjoa*

Secrecy Forever? Analysis of Anonymity in Internet-Based Voting Protocols \_\_\_\_\_ 340  
*Melanie Volkamer and Robert Krimmer*

A Practical Framework for Dynamically Immunizing Software Security Vulnerabilities \_\_\_\_\_ 348  
*Zhiqiang Lin, Bing Mao, and Li Xie*

### **Session 11: Security Management**

A Study of Security Architectural Patterns \_\_\_\_\_ 358  
*David García Rosado, Carlos Gutiérrez, Eduardo Fernández-Medina, and Mario Piattini*

Workshop-Based Multiobjective Security Safeguard Selection \_\_\_\_\_ 366  
*Thomas Neubauer, Christian Stummer, and Edgar Weippl*

Towards a Security Architecture for Vehicular Ad Hoc Networks \_\_\_\_\_ 374  
*Klaus Plöbfl, Thomas Nowey, and Christian Mletzko*

Improving Security Management through Passive Network Observation \_\_\_\_\_ 382  
*Yohann Thomas, Hervé Debar, and Benjamin Morin*

Digital Signatures for Modifiable Collections \_\_\_\_\_ 390  
*Serge Abiteboul, Bogdan Cautis, Amos Fiat, and Tova Milo*

### **Session 12: Distributed Systems**

A System Architecture for Enhanced Availability of Tightly Coupled Distributed Systems \_\_\_\_\_ 400  
*Johannes Osrael, Lorenz Frohofer, Karl M. Goeschka,  
Stefan Beyer, Pablo Galdámez, and Francesc Muñoz*

DeDiSys Lite: An Environment for Evaluating Replication Protocols in  
Partitionable Distributed Object Systems \_\_\_\_\_ 408  
*Stefan Beyer, Alexander Sánchez, Francesc Muñoz-Escó, and Pablo Galdámez*

Defense Trees for Economic Evaluation of Security Investments \_\_\_\_\_ 416  
*Stefano Bistarelli, Fabio Fioravanti, and Pamela Peretti*

Proposed Framework for Achieving Interoperable Services between European Public Administrations \_\_\_\_\_ 424  
*Amir Hayat, Muhammad Alam, and Thomas Rössler*

Gait Recognition Using Acceleration from MEMS \_\_\_\_\_ 432  
*Davronzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol*

### **Session 13: Software Security and Dependability**

Making Web Services Dependable \_\_\_\_\_ 440  
*Louise Moser, P. Michael Melliar-Smith, and Wenbing Zhao*

A Simple Component Connection Approach for Fault Tree Conversion to Binary Decision Diagram \_\_\_\_\_ 449  
*John Andrews and Rasa Remenyte*

Secure Business Process Management: A Roadmap \_\_\_\_\_ 457  
*Thomas Neubauer, Markus Klemen, and Stefan Biffel*



Supporting Attribute-Based Access Control with Ontologies \_\_\_\_\_ 465  
*Torsten Priebe, Wolfgang Dobmeier, and Nora Kamprath*

Diagnosis of Complex Systems Using Ant Colony Decision Petri Nets \_\_\_\_\_ 473  
*Calin Ciufudean, Adrian Graur, Constantin Filote, Cornel Turcu, and Valentin Popa*

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

### **Session 1: IP Network and Adhoc Network**

A Lightweight Model of Trust Propagation in a Multi-Client Network Environment:  
To What Extent does Experience Matter? \_\_\_\_\_ 482  
*Marc Conrad, Tim French, Wei Huang, and Carsten Maple*

Secure 3G User Authentication in Adhoc Serving Networks \_\_\_\_\_ 488  
*Arjan Durrresi, Lyn Evans, Vamsi Paruchuri, and Leonard Barolli*

Security Analysis for IP-Based Government Emergency Telephony Service \_\_\_\_\_ 496  
*Feng Cao and Saadat Malik*

Inter-Domains Security Management Model (IDSM) for IP Multimedia Subsystem (IMS) \_\_\_\_\_ 502  
*Muhammad Sher, Thomas Magedanz, and Walter T. Penzhorn*

Privacy Threats and Issues in Mobile RFID \_\_\_\_\_ 510  
*Hyangjin Lee and Jeeyeon Kim*

### **Session 2: Wireless and Sensor Network**

A Framework of Survivability Model for Wireless Sensor Network \_\_\_\_\_ 515  
*Dong Seong Kim, Khaja Mohammad Shazzad, and Jong Sou Park*

Mitigating Denial of Service Threats in GSM Networks \_\_\_\_\_ 523  
*Valer Bocan and Vladimir Creţu*

Achieving Availability and Reliability in Wireless Sensor Networks Applications \_\_\_\_\_ 529  
*Amirhosein Taherkordi, Majid Alkaee Taleghan, and Mohsen Sharifi*

Secure Enhanced Wireless Transfer Protocol \_\_\_\_\_ 536  
*Jin-Cherng Lin, Yu-Hsin Kao, and Chen-Wei Yang*

### **Session 3: Authentication and Authorization**

Quality of Password Management Policy \_\_\_\_\_ 544  
*Carlos Villarrubia, Eduardo Fernández-Medina, and Mario Piattini*

A Proposal of an Anonymous Authentication Method for Flat-rate Service \_\_\_\_\_ 551  
*Yoshio Kakizaki, Hiroshi Yamamoto, and Hidekazu Tsuji*

Recovery Mechanism of Online Certificate Chain in Grid Computing \_\_\_\_\_ 558  
*MingChu Li, Jianbo Ma, and Hongyan Yao*

#### **Session 4: Trust Management and Recovery**

- PKI Trust Relationships: From a Hybrid Architecture to a Hierarchical Model \_\_\_\_\_ 563  
*Cristina Satizábal, Rafael Páez, and Jordi Forné*
- Recovery Mechanism of Cooperative Process Chain in Grid \_\_\_\_\_ 571  
*MingChu Li and Hongyan Yao*
- Run Time Detection of Covert Channels \_\_\_\_\_ 577  
*Naoyuki Nagatou and Takuo Watanabe*

#### **Session 5: Secure Information System**

- Practical Approach of a Secure Management System Based on ISO/IEC 17799 \_\_\_\_\_ 585  
*Luis Enrique Sánchez, Daniel Villafranca, Eduardo Fernández-Medina, and Mario Piattini*
- Testing Complex Business Process Solutions \_\_\_\_\_ 593  
*Gerd Saurer, Josef Schiefer, and Alexander Schatten*
- Deontic Relevant Logic as the Logical Basis for Specifying, Verifying, and Reasoning about  
Information Security and Information Assurance \_\_\_\_\_ 601  
*Jingde Cheng and Junichi Miura*
- Resource Management Continuity with Constraint Inheritance Relation \_\_\_\_\_ 609  
*Zude Li, Guoqiang Zhan, and Xiaojun Ye*

#### **Session 6: Availability**

- On the Reliability of Web Clusters with Partial Replication of Contents \_\_\_\_\_ 617  
*Jose Daniel Garcia, Jesus Carretero, Felix Garcia,  
Alejandro Calderon, Javier Fernandez, and David E. Singh*
- Reliability Modeling Strategy of an Industrial System \_\_\_\_\_ 625  
*Syed Rizwan and Ramachandran KP*
- Persistent Computing Systems as Continuously Available, Reliable, and Secure Systems \_\_\_\_\_ 631  
*Jingde Cheng*
- Active/Active Replication for Highly Available HPC System Services \_\_\_\_\_ 639  
*Christian Engelmann, Stephen L. Scott, Chokchai "Box" Leangsuksun, and Xubin (Ben) He*

#### **Session 7: Software Security 1**

- Towards an Integrated Conceptual Model of Security and Dependability \_\_\_\_\_ 646  
*Erland Jonsson*
- A Comparison of the Common Criteria with Proposals of Information Systems Security Requirements \_\_\_\_\_ 654  
*Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini*
- Secure and Reliable Java-Based Middleware — Challenges and Solutions \_\_\_\_\_ 662  
*Walter Binder*

## Session 8: Software Security 2

Security Requirement with a UML 2.0 Profile _____	670
<i>Alfonso Rodriguez, Eduardo Fernández-Medina, and Mario Piattini</i>	
Representing Levels of Abstraction to Facilitate the Secure Multidimensional Modeling _____	678
<i>Rodolfo Villarroel, Emilio Soler, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini</i>	
Modeling Permissions in a (U/X)ML World _____	685
<i>Muhammad Alam, Ruth Breu, and Michael Hafner</i>	

## Session 9: Safety and Security

Application of the Digraph Method in System Fault Diagnostics _____	693
<i>Emma Kelly and Lisa Bartlett</i>	
No Risk is Unsafe: Simulated Results on Dependability of Complementary Currencies _____	701
<i>Kenji Saito, Eiichi Morino, and Jun Murai</i>	

## Session 10: E-commerce and E-Government

A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce _____	709
<i>Christian Schläger, Thomas Nowey, and Jose A. Montenegro</i>	
Achieving Fairness and Timeliness in a Previous Electronic Contract Signing Protocol _____	717
<i>Magdalena Payeras-Capellà, Josep Lluís Ferrer-Gomila, and Llorenç Huguet-Rotger</i>	
Digital Signatures with Familiar Appearance for e-Government Documents: <i>Authentic PDF</i> _____	723
<i>Thomas Neubauer, Edgar Weippl, and Stefan Biffi</i>	

## Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)

### Session 1: Construction of Dependable Overlay Networks

Efficient Link Failure Detection and Localization using P2P-Overlay Networks _____	732
<i>Barbara Emmert and Andreas Binzenhöfer</i>	
Replication Strategies for Reliable Decentralised Storage _____	740
<i>Matthew Leslie, Jim Davies, and Todd Huffman</i>	

### Session 2: Security

Multipath Key Exchange on P2P Networks _____	748
<i>Yuuki Takano, Naoki Isozaki, and Yoichi Shimoda</i>	
Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration _____	756
<i>Jochen Dinger and Hannes Hartenstein</i>	

### Session 3: Social Front

Fair Trading of Information: A Proposal for the Economics of Peer-to-Peer Systems _____	764
<i>Kenji Saito, Eiichi Morino, and Jun Murai</i>	
Ecosystem of Naming Systems: Discussions on a Framework to Induce Smart Space Naming Systems Development _____	772
<i>Yusuke Doi, Shirou Wakayama, Masahiro Ishiyama, Satoshi Ozaki, Tomohiro Ishihara, and Yojiro Uo</i>	
Deriving Ratings through Social Network Structures _____	779
<i>Omer Rana, Hameeda Alshabib, and Ali ShaikhAli</i>	

### Workshop on Bayesian Networks in Dependability (BND2006)

Bayesian Networks Implementation of the Dempster Shafer Theory to Model Reliability Uncertainty _____	788
<i>Christophe Simon and Philippe Weber</i>	
Multi-Agent Causal Models for Dependability Analysis _____	794
<i>Sam Maes and Philippe Leray</i>	
Computing Multiple Diagnoses in Large Devices Using Bayesian Networks _____	799
<i>Véronique Delcroix, Mohamed-Amine Maalej, and Sylvain Piechowiak</i>	
Automatically Translating Dynamic Fault Trees into Dynamic Bayesian Networks by Means of a Software Tool _____	804
<i>Stefania Montani, Luigi Portinale, Andrea Bobbio, and Daniele Codetta-Raiteri</i>	
Modelling the Reliability of Search and Rescue Operations within the UK through Bayesian Belief Networks _____	810
<i>Ashley Russell, John Quigley, and Robert van der Meer</i>	
Modelling Dependable Systems Using Hybrid Bayesian Networks _____	817
<i>Martin Neil, Manesh Tailor, David Marquez, Norman Fenton, and Peter Hearty</i>	

### Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)

An Architecture for Service Discovery Based on Capability Matching _____	824
<i>Jaka Močnik and Piotr Karwaczynski</i>	
A Declarative Control Language for Dependable XML Message Queues _____	832
<i>Alexander Böhm, Carl-Christian Kanne, and Guido Moerkotte</i>	
Timed Modelling and Analysis in Web Service Compositions _____	840
<i>Raman Kazhamiakin, Paritosh Pandya, and Marco Pistore</i>	
Web Service Discovery, Replication, and Synchronization in Ad-Hoc Networks _____	847
<i>Lukasz Juszczak, Jaroslaw Lazowski, and Schahram Dustdar</i>	
Evaluating Certification Protocols in the Partial Database State Machine _____	855
<i>António Sousa, Alfrânio Correia Jr, Francisco Moura, José Pereira, and Rui Oliveira</i>	

### **Workshop: Security in E-Learning (SEL)**

A Secure E-Exam Management System _____	864
<i>Jordi Castellà-Roca, Jordi Herrera-Joancomarti, and Aleix Dorca-Josa</i>	
Intra-Application Partitioning in an eLearning Environment — A Discussion of Critical Aspects _____	872
<i>Elke Franz and Katrin Borcea-Pfzmann</i>	
Access Control in a Privacy-Aware eLearning Environment _____	879
<i>Elke Franz, Hagen Wahrig, Alexander Boettcher, and Katrin Borcea-Pfzmann</i>	
Adding Security to a Multiagent Learning Platform _____	887
<i>Carine Webber, Maria de Fátima W. do Prado Lima, Marcos E. Casa, and Alexandre M. Ribeiro</i>	
Unlocking Repositories: Federated Security Solution for Attribute and Policy Based Access to Repositories via Web Services _____	895
<i>Marek Hatala, Ty Mey (Timmy) Eap, and Ashok Shah</i>	

### **Workshop "Dependability Aspects on Data Warehousing and Mining Applications (DAWAM 2006)**

Offline Internet Banking Fraud Detection _____	904
<i>Vasilis Aggelis</i>	
Practical Approaches for Analysis, Visualization and Destabilizing Terrorist Networks _____	906
<i>Nasrullah Memon and Henrik Legind Larsen</i>	
Representing Security and Audit Rules for Data Warehouses at The Logical Level by Using the Common Warehouse Metamodel _____	914
<i>Emilio Soler, Juan Trujillo, Rodolfo Villaroel, Eduardo Fernández-Medina, and Mario Piattini</i>	
A 2 <sup>d</sup> -Tree-Based Blocking Method for Microaggregating Very Large Data Sets _____	922
<i>Agusti Solanas, Antoni Martínez-Ballesté, Josep Domingo-Ferrer, and Josep M. Mateo-Sanz</i>	
Using a Bayesian Averaging Model for Estimating the Reliability of Decisions in Multimodal Biometrics _____	929
<i>Vitaly Schetinin and Carsten Maple</i>	
On Efficiency and Data Privacy Level of Association Rules Mining Algorithms within Parallel Spatial Data Warehouse _____	936
<i>Marcin Gorawski and Karol Stachurski</i>	
Dependability in Data Mining: A Perspective from the Cost of Making Decisions _____	944
<i>H. Michael Chung</i>	

### **Workshop on Bioinformatics and Security (BIOS 06)**

Grid Infrastructures for Secure Access to and Use of Bioinformatics Data: Experiences from the BRIDGES Project _____	950
<i>Richard Sinnott, M. Bayer, A. Stell, and J. Koetsier</i>	
The Usability and Practicality of Biometric Authentication in the Workplace _____	958
<i>Carsten Maple and Peter Norrington</i>	
Building an Encrypted File System on the EGEE Grid: Application to Protein Sequence Analysis _____	965
<i>Christophe Blanchet, G. Deléage, and R. Mollon</i>	

**Workshop: Information Security Risk Management (ISRM)**

The Knowledge Pressure on Risk and Security Managers is Increasing \_\_\_\_\_ 974  
*Christer Magnusson, Heidi Olá, and Camilla Silversjö Holmqvist*

Validation of IT-Security Measurement Tools \_\_\_\_\_ 980  
*Ruedi Baer and Martin Dietrich*

Risk Management Approach on Identity Theft in Biometric Systems Context \_\_\_\_\_ 982  
*Sabine Delaitre*

**Workshop "Dependability and Security in e-Government" (DeSeGov 2006)**

E-voting: Dependability Requirements and Design for Dependability \_\_\_\_\_ 988  
*Jeremy Bryans, Bev Littlewood, Peter Ryan, and Lorenzo Strigini*

Defining Criteria for Rating an Entity's Trustworthiness Based on Its Certificate Policy \_\_\_\_\_ 996  
*Omar Batarfi and Lindsay Marshall*

A Component Based Software Architecture for E-Government Applications \_\_\_\_\_ 1004  
*Raphael Kunis, Daniel Beer, and Gudula Runger*

Designing Mutual-aid Model for RAQ (Rarely Asked Question) in e-Government:  
Practical use of Anonymity \_\_\_\_\_ 1012  
*Akiko Orita*

Maintaining Data-Integrity in the Back Office Registries of Cities;  
A Survey on Organizational Barriers and Ways to Address Those \_\_\_\_\_ 1017  
*Rob Peters, Marco Meesters, Pim Jorg, Edwin Stuart, and Marcel Hoogwout*

Choosing the Right Wireless LAN Security Protocol for the Home and Business User \_\_\_\_\_ 1025  
*Carsten Maple, Helen Jacobs, and Matthew Reeve*

An Ontology for Secure e-Government Applications \_\_\_\_\_ 1033  
*M. Karyda, T. Balopoulos, S. Dritsas, L. Gymnopoulos,  
S. Kokolakis, C. Lambrinouidakis, and S. Gritzalis*

Building Governments in e-Government: Settlement of Trusted e-Oligarchy \_\_\_\_\_ 1038  
*Semir Daskapan*

**Author Index \_\_\_\_\_ 1045**

# Message from the Organizing Committee

The idea for this conference came from the colleagues of the various ARES 2006 committees; our goal being to build a bridge amongst the various aspects of system dependability as an integrated concept.

The idea to launch the conference in Austria in the first half of the year 2006 has also to do with Austria's Presidency of the European Union from January to June 2006.

The European Union and the Austrian Governmental Bodies are very keen to bridge the gap between the scientific work and applications in this area — especially in the areas of e-Government.

We are very pleased therefore to have this conference organised in cooperation with ENISA (The European Network and Information Security Agency). ENISA supports the idea of this conference due to the urgent need of research and dissemination of new techniques in this key area.

We hope that the conference will have a real benefit for innovative applications which have to consider the various dependability issues, and furthermore will build a platform for in-depth discussions between researchers in the different areas of Dependability such as Availability, Reliability, and Security.

We received 159 papers from 35 countries for ARES and the Program Committee eventually selected 58 papers, making an acceptance rate of 36.47 percent of submitted papers.

Eight workshops are organised on special topics of ARES, i.e.:

- Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)
- Workshop on Bayesian Networks in Dependability (BND2006)
- Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)
- Workshop: Security in E-Learning (SEL)
- Workshop "Dependability Aspects on Data Warehousing and Mining Applications" (DAWAM 2006)
- Workshop on Bioinformatics and Security (BIOS 06)
- Workshop: Information Security Risk Management (ISRM)
- Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

As an additional feature of ARES we have invited distinguished scientists for the International Symposium on Frontiers in Availability, Reliability and Security (FARES) to present and discuss special aspects relevant for future applications and research.

We would like to express our gratitude to all program committee members, workshop organisers and committee members and all the external referees who reviewed the papers very thoroughly and in a timely manner.

Due to the high number of submissions and the quality of the submitted papers, the reviewing, and discussion process was an extraordinarily challenging task. In total they have dealt with 232 papers.

Special thanks must be given to Mr. Tho Manh Nguyen for all his support in the organization of the PC-tasks of ARES 2006 and workshop coordination. We would also like to thank all the authors who submitted their papers to ARES 2006.

Finally many thanks to Ms. Christine Tronigger for providing a great deal of support in administering the registrations.

**Prof. Norman Revell, Prof. Roland Wagner (Honorary Co-chairs)**  
**Prof. Günther Pernul, Prof. Makoto Takizawa (General Co-chairs)**  
**Prof. Gerald Quirchmayr, Prof. A Min Tjoa (Program Co.-chairs)**

# **ARES and Workshops Committees**

## **Honorary Co-Chairs**

Norman Revell, Middlesex University, United Kingdom  
Roland Wagner, University of Linz, Austria

## **General Co-Chairs**

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

## **Program Co-Chairs**

Gerald Quirchmayr, University of Southern Australia, Australia  
A Min Tjoa, Vienna University of Technology, Austria

## **Workshops Co-Chairs**

Nguyen Manh Tho, Vienna University of Technology, Austria  
Abdelkader Hameurlain, University of Toulouse, France  
Leonard Barolli, Fukuoka Institute of Technology (FIT), Japan

## **International Liaison Chair**

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

## **Publicity Chair**

Vladimir Marik, Czech Technical University, Czech Republic

## **Publication Chair**

Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway

## **Local Organizing Co-Chairs**

Maria Schweikert, Vienna University of Technology, Austria  
Markus Klemen, Vienna University of Technology, Austria

## **Program Committee**

Jemal Abawajy, Deakin University, Australia  
Abiola Abimbola, Napier University, UK  
Rafael Accorsi, University of Freiburg, Germany  
Alessandro Acquisti, Carnegie Mellon University, USA  
John Andrews, Loughborough University, UK  
Lisa Bartlett, Loughborough University, UK  
Elisa Bertino, Purdue University, USA  
Bharat Bhargava, Purdue University, USA  
Stefan Biffel, Vienna University of Technology, Austria  
Michael Burmester, Florida State University, USA  
Jiannong Cao, Hong Kong Polytechnic University, Hongkong, China  
Jordi Castellà-Roca, Rovira i Virgili University of Tarragona  
Anirban Chakrabarti, Infosys Technologies, India  
Guihai Chen, Nanjing University, China  
John A. Clark, University of York, UK  
George Davida, University of Wisconsin Milwaukee, USA  
Pierpaolo Degano, Università di Pisa, Italia  
Robert Deng, Singapore Management University, Singapore  
Yvo Desmedt, University College London, UK



Zoran Despotovic, DoCoMo Euro-Labs, Germany  
 Roger Dingledine, The Free Haven Project, USA  
 Paolo Donzelli, Office of the Prime Minister, Italy  
 Jeroen Doumen, University of Twente, Neitherland  
 Schahram Dustdar, Vienna University of Technology, Austria  
 Gerhard Eschelbeck, Webroot Inc., USA  
 Yung-Chin Fang, Dell Corp., USA  
 Pascal Felber, Université de Neuchâtel, Switzerland  
 Elena Ferrari, Universita' dell' Insubria, Italy  
 Jordi Forné, Universitat Politècnica de Catalunya, Spain  
 Felix C. Freiling, RWTH Aachen University, Germany  
 Steven Furnell, University of Plymouth, UK  
 Stephan Groß, Technische Universität Dresden, Germany  
 Daniel Grosu, Wayne State University, USA  
 Yong Guan, Iowa State University, USA  
 Ibrahim Haddad, Concordia University, Canada  
 Abdelkader Hameurlain, Université Paul Sabatier, France  
 Marit Hansen, Independent Centre for Privacy Protection Schleswig-Holstein Kiel, Germany  
 Naohiro Hayashibara, Tokyo Denki University, Japan  
 Xubin (Ben) He, Tennessee Technological University, USA  
 Yanxiang He, Wuhan University, China  
 Rattikorn Hewett, Texas Tech University, USA  
 Jimmy Huang, York University, Canada  
 Jan Jürjens, Munich University of Technology, Germany  
 Erland Jonsson, Chalmers University of Technology, Sweden  
 Oliver Jorns, ftw. Forschungszentrum Telekommunikation Wien, Austria  
 Audun Josang, University of Queensland, Australia  
 Yukiko Kawai, National Institute of Information and Communications Technology, Japan  
 Dogan Kesdogan, RWTH Aachen Informatik IV, Germany  
 Hiroaki Kikuchi, Tokai University, Japan  
 Hong Ong Oak, Ridge National Laboratory, USA  
 Seungjoo Kim, Sungkyunkwan University, Korea  
 Christian Kirchsteiger, European Commission  
 Peter Küng, Credit Suisse, Switzerland  
 Sy-Yen Kuo, National Taiwan UniversityTaiwan, R.O.C  
 Marc Lacoste, France Télécom Division R&D., France  
 Kwok-Yan Lam, Tsinghua University, China  
 Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway  
 Chokchai (Box) Leangsuksun, Louisiana Tech University, USA  
 Yih-Jiun Lee, Chienkuo Technology University, Taiwan, R.O.C  
 Chin-Laung Lei, National Taiwan University, R.O.C  
 Chae Hoon Lim, Sejong University, Korea  
 Ching Lin, Macquarie University, Australia  
 Tong Liu, Dell Corp., USA  
 Javier Lopez, University of Malaga, Spain  
 Sanlu Lu, Nanjing University, China  
 Burgazzi Luciano, ENEA, Italy  
 Jianhua Ma, Hosei University, Japan  
 Josef Makolm, Federal Ministry of Finance, Austria  
 Geyong Min, University of Bradford, UK  
 Yi Mu, University of Wollongong, Australia  
 Günter Müller, Telematik Universitaet Freiburg, Germany  
 Junghyun Nam, Sungkyunkwan University, Korea  
 Tho Manh Nguyen, Vienna University of Technology, Austria  
 Jesper Buus Nielsen, Aarhus University, Denmark  
 Flemming Nielson, Technical University of Denmark, Denmark

Juan Gonzalez Nieto, Queensland University of Technology, Australia  
Thomas Nowey, University of Regensburg, Germany  
Manish Parashar, Rutgers University, USA  
Fernando Pedone, Universita della Svizzera Italiana, Switzerland  
María S. Pérez-Hernández, Universidad Politécnica de Madrid, Spain  
Mario Piattini, University of Castilla La Mancha, Spain  
Makan Pourzandi, Ericsson Inc.  
Christopher Price, University of Wales Aberystwyth, UK  
Philipp Reisner, MD at LINBIT Information Technologies GmbH, Austria  
Heiko Rosnagel, Johann Wolfgang Goethe University Frankfurt, Germany  
Bimal Roy, Indian Statistical Institute, India  
Rei Safavi-Naini, University of Wollongong, Australia  
Kenji Saito, Keio University, Japan  
Kouichi Sakurai, Kyushu University, Japan  
Henrique Santos, Universidade do Minho, Portugal  
Stephen L. Scott, Oak Ridge National Laboratory  
Jean-Marc Seigneur, University of Geneva, Switzerland  
Ahmed Serhrouchni, Telecom Paris, France  
Ingrid Schaumüller-Bichl, ITSB Linz, Austria  
Charles Shoniregun, University of East London, UK  
Amund Skavhaug, Norwegian University of Science and Technology (NTNU), Norway  
Neal A. Snooke, University of Wales Aberystwyth, UK  
Ketil Stølen, SINTEF and University of Oslo, Norway  
Peter Struss, Technische Universität und Occ'm Software, Germany  
Tsuyoshi Takagi, FutureUniversity – Hakodate, Japan  
Makoto Takizawa, Tokyo Denki University, Japan  
A Min Tjoa, Vienna University of Technology, Austria  
Jorge Villar, Universitat Politècnica de Catalunya, Spain  
Roland Wagner, University of Linz, Austria  
Edgar Weippl, Vienna University of Technology, Austria  
Chuan-Kun Wu, Chinese Academy of Sciences, China  
Cheng-Zhong Xu, Wayne State University, USA  
Mariemma I. Yagüe, University of Malaga, Spain  
Laurence T. Yang, St. Francis Xavier University, Canada  
Alec Yasinsac, Florida State University, USA  
George Yee, National Research Council, Canada  
Sung-Ming Yen, National Central University, Taiwan, R.O.C  
Bill Yurcik, National Center for Supercomputing Applications (NCSA)  
Nicola Zannone, University of Trento, Italy  
Jianhong Zhang, North China University of Technology, China  
Jianying Zhou, Institute for Infocomm Research, Singapore  
Huafei Zhu, Institute for Infocomm Research, Singapore

## **Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)**

### **Workshop Organizers**

Yusuke Doi, Toshiba Corporation, Japan  
Youki Kadobayashi, Nara Institute of Science and Technology, Japan  
Kenji Saito, Graduate School of Media and Governance, Keio University, Japan

### **Program Committee**

Stéphane Bressan, National University of Singapore, Singapore  
Bernard Burg, Panasonic Research, USA  
Ian Clarke, Freenet Project, UK  
Roger Dingledine, The Free Haven Project, USA  
Yusuke Doi, Toshiba Corporation, Japan (co-chair)  
Claudiu Duma, Linköping University, Sweden  
Debojyoti Dutta, University of Southern California, USA  
Noria Foukia, University of Otago, New Zealand  
Maria Gini, University of Minnesota, USA  
Achmad Nizar Hidayanto, University of Indonesia, Indonesia  
Sam Joseph, University of Hawaii, USA  
Youki Kadobayashi, Nara Institute of Science and Technology, Japan (co-chair)  
Anirban Mondal, University of Tokyo, Japan  
Akiko Orita, Keio University, Japan  
Omer F. Rana, Cardiff University, UK  
Kenji Saito, Keio University, Japan (co-chair)  
Claudio Sartori, University of Bologna, Italy  
Nguyen Manh Tho, Vienna University of Technology, Austria  
Sheng Zhong, State University of New York at Buffalo, USA

## **Workshop on Bayesian Networks in Dependability (BND2006)**

### **Workshop Co-chairs**

Stefania Montani, University of Piemonte Orientale  
Hichem Boudali, University of Twente

### **Workshop Committee**

Joanne Bechta Dugan, University of Virginia  
Marc Bouissou, Electricite' de France  
Helge Langseth, Sintef, Norway  
Luigi Portinale, University of Piemonte Orientale  
John L. Quigley, University of Strathclyde, Glasgow  
Luis E. Sucar, Department of Computer Science, INAOE, Puebla, Mexico  
Philippe Weber, Université Henri Poincaré, Nancy

## **Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS 2006)**

### **Program Chairs**

Karl M. Göschka, Vienna University of Technology, Austria  
Schahram Dustdar, Vienna University of Technology, Austria  
Mehdi Jazayeri, University of Lugano, Switzerland

### **Organizational Chair**

Martin Treiber, Vienna University of Technology, Austria

### **Program Committee**

Marco Aiello, University of Trento, Italy  
Mikio Aoyama, Nanzan University, Japan  
Luciano Baresi, Politecnico di Milano, Italy  
Boualem Benatallah, UNSW, Australia  
Sara Bouchenak, University of Grenoble I, France  
Sjaak Brinkkemper, Univ. of Utrecht, Netherlands  
Tevfik Bultan, University of California, USA  
Fabio Casati, HP, USA  
Malu Castellanos, Hewlett-Packard, USA  
Gianpaolo Cugola, Italy  
Harmke de Groot, Netherlands  
Asuman Dogac, METU, Turkey  
Dieter Fensel, DERI, Ireland  
Gianluigi Ferrari, University of Pisa, Italy  
Jacqueline Floch, Sintef, Norway  
Kary Fraemling, Helsinki University of Technology, Finland  
Claude Godart, INRIA, France  
Paul Grefen, Eindhoven Uni. of Technology, Netherlands  
John Grundy, University of Auckland, New Zealand  
Mohand-Said Hacid, Universite Claude Bernard Lyon, France  
Manfred Hauswirth, EPFL, Switzerland  
Alfons Kemper, TU Muenchen, Germany  
Bernd Kraemer, University of Hagen, Germany  
Frank Leymann, University of Stuttgart, Germany  
Ozelin Lopez, ATOS Origin, Spain  
Brahim Medjahed, University of Michigan, USA  
Joachim Nern, Aspasia Systems, Germany  
Beng Chin Ooi, National University of Singapore, Singapore  
Maria Orłowska, UQ, Australia  
Aris M. Ouksel, University of Illinois at Chicago, USA  
Mike Papazoglou, Tilburg Univ., Netherlands  
Jose Pereira, Universidade do Minho, Portugal  
Barbara Pernici, Politecnico di Milano, Italy  
Marco Pistore, Università di Trento, Italy  
Dimitris Plexousakis, FORTH, Greece  
Alexander Romanovsky, University of Newcastle, UK  
Anne-Marie Sassen, European Commission, EU  
Vladimiro Sassone, University of Sussex, UK  
Ian Sommerville, Lancaster University, UK  
Jianwen Su, UCSB, USA  
Katia Sycara, Carnegie Mellon University, USA  
Stefan Tai, IBM Watson, USA  
Paolo Traverso, ITC, Italy  
Elena Troubitsyna, Aabo Akademi, Finland  
Wil van der Aalst, Eindhoven University of Technology, Netherlands

Jos van Hillegersberg, Univ. of Twente, Netherlands  
Steve Vinoski, IONA, USA  
Martin Wirsing, Ludwig-Maximilians-University Munich, Germany  
Jian Yang, Macquarie University, Australia  
Gianluigi Zavattaro, University of Bologna, Italy

**Workshop: Security in E-Learning (SEL)**

**Program Chair**

Edgar Weippl, Vienna University of Technology, Austria

**Program Committee**

Elke Franz, Dresden University of Technology, Germany  
Gerald Quirchmayr, University of South Australia, Australia  
Tomaz Klobucar, Jozef Stefan Institute, Slovenija  
Günther Pernul, University of Regensburg, Germany

**Workshop "Dependability Aspects on Data Warehousing and Mining Applications" (DAWAM 2006)**

**Organizer Co-chairs**

Jimmy Huang, York University, Canada  
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria  
Nguyen Manh Tho, Vienna University of Technology, Austria

**Program Committee**

Jernal Abawajy, Deakin University, Australia  
Aijun An, York University, Canada  
Pawan Chowdhary, IBM T J Watson Research Center, USA  
LiWu Chang, Naval Research Laboratory, USA  
Josep Domingo-Ferrer, Rovira i Virgili University of Tarragona, Spain  
Elena Ferrari, University of Insubria at Como, Italy  
Ulrich Flegel, University of Dortmund, Germany  
Tyrone Grandison, IBM Almaden Research, USA  
Jimmy Huang, York University, Canada  
Jun-Jang (JJ) Jeng, IBM T.J. Watson Research Center, USA  
Hillol Kargupta, University of Maryland, Baltimore County, USA and Agnik, LLC  
Zongwei Luo, University of Hong Kong, Hong Kong  
Taneli Mielikäinen, University of Helsinki, Finland  
Tho Manh Nguyen, Vienna University of Technology, Austria  
Daniel E. O'Leary, University of Southern California, USA  
Stanley Oliveira, Embrapa Information Technology, Brazil  
Arnon Rosenthal, MITRE Corporation, USA  
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria  
Ben Soh, La Trobe University, Australia  
David Taniar, Monash University, Australia  
Juan Trujillo, University of Alicante, Spain  
Vassilios S. Verykios, University of Thessaly, Greece  
Justin Zhan, University of Ottawa, Canada  
Sheng Zhong, State University of New York at Buffalo, USA

## **Workshop on Bioinformatics and Security (BIOS 06)**

### **Workshop Chairs**

Küng Josef, University of Linz, FAW Austria  
Mazuran Petra, FAW, Austria  
Wagner Roland, University of Linz, FAW Austria

### **Program Committee**

Eisenacher Martin, University of Münster, Germany  
Hochreiter Sepp, TU Berlin, Germany  
Hof Sonja, (DWS) AG, Switzerland  
Kramer Stefan, TUM, Germany  
Marik Vladimir, Technical University Prag, Czech  
Mazuran Petra, FAW, Austria  
Palkoska Jürgen, FAW Austria  
Retschitzegger Werner, University of Linz, Austria  
Revell Norman, Middlesex University, UK  
Tjoa A Min, Technical University of Vienna, Austria

## **Workshop: Information Security Risk Management (ISRM)**

### **Workshop Chairs**

Professor Dr. D. Karagiannis, University of Vienna, Austria  
Dr. L. Marinos, ENISA, Greece

### **Program Committee**

M. Dietrich, BSG Unternehmensberatung, Switzerland  
M. Hoevers, ECP-NL, Platform voor eNetherlands, The Netherlands  
K. Kalmelid, Swedish Emergency Management Agency, Sweden  
S. Lebel, Dir. Centrale de la Sécurité des Systèmes d'information, France  
Prof. Dr. G. Müller, Telematik, Univ. of Feiburg, Germany  
M. Rohde, European Commission, DG Information Society and Media, Belgium  
Dr. I. Schaumüller-Bichl, IT Security Consultant, Austria

## **Workshop "Dependability and Security in e-Government" (DeSeGov 2006)**

### **Workshop Chairs**

A Min Tjoa, Vienna University of Technology, Austria  
Erich Schweighofer, University of Vienna, Austria

### **Program Committee**

Peggy Agouris, University of Maine, USA  
Yigal Arens, USC/Columbia University Digital Government Research Center, USA  
Jon Bing, University of Oslo, Norway  
Fernando Galindo, University of Zaragoza, Spain  
Dieter Klumpp, Alcatel SEL Foundation, Germany  
Robert Krimmer, Vienna University of Economics and Business Administration, Austria  
Scott F. Midkiff, Virginia Polytechnic Institute and State University, USA  
Enrico Nardelli, University of Rome Tor Vergata, Italy  
Tho Manh Nguyen, Vienna University of Technology, Austria  
Erich Schweighofer, University of Vienna, Austria  
Efthimios Tambouris, CERTH/ITI, Greece  
A Min Tjoa, Vienna University of Technology, Austria  
Greg B. White, The University of Texas at San Antonio, USA  
Maria A. Wimmer, University of Koblenz, Germany

# Quality of Password Management Policy

Carlos Villarrubia, Eduardo Fernández-Medina and Mario Piattini  
*Alarcos Research Group*  
*Information Systems and Technologies Department*  
*UCLM-Soluziona Research and Development Institute*  
*University of Castilla-La Mancha*  
*Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain*  
*{Carlos.Villarrubia, Eduardo.FdezMedina, Mario.Piattini}@uclm.es*

## Abstract

*The use of passwords is the most common method to carry out the authentication of users in information systems. For this reason, quality in the password management is a need to reach reasonable levels in the typical objectives of security. In this paper, we propose a set of metrics of password policies based on the most outstanding factors in this authentication mechanism. Together with the metrics, we propose a quality indicator derived from these metrics that allows us to have a global vision of the quality of the password management policy used. Finally, we will indicate the future works to be performed to check the validity and usefulness of the proposed metrics.*

## 1. Introduction

The use of an authentication system requires the integration of multiple elements; depending on the used techniques, it is necessary to use cryptography, medicine, psychology, systems analysis and protocol design. All authentication systems are designed to assure the identity of a participant to other participant and this process requires that the first participant demonstrates his identity according to any kind of information (knowledge evidence, possession evidence, and biological evidence). This authentication evidence can be a word or a password as it is used in the majority of operating systems and applications (knowledge evidence), a cryptographic card (possession evidence) or any biological characteristic of the individual to be authenticated and that is measured through a biometric device (biological evidence).

Historically, the use of a mechanism based on passwords has been the most used method. The importance of this authentication mechanism has led to

the elaboration of rules and recommendations of multiple levels [11, 12, 13, 14, 20, 21]. The fact that this method is very easy to use in all systems together with its low cost has motivated this acceptance [18]. Deficiencies of this method have been widely studied and measures have been proposed to limit these disadvantages [2, 9, 23]. In some designs, the main disadvantages are linked to the necessary confidence in users when dealing with passwords while in other occasions, these disadvantages are motivated by designs that assumed a secure environment (such as, intranets) and that have been used in other environments (for example, the Internet) [10].

All these problems should indicate that passwords are a mechanism to be replaced but the users' acceptance of their use, their low cost together with the complexity and costs of the alternative methods guarantee their short and medium term continuance.

### 1.1 Security Metrics

Information and its support processes together with systems and nets are important resources for any organization. These resources are continuously subjected to risks and insecurities coming from a great variety of sources, where there are threats based on malicious code, programming errors, human errors, sabotages or fires.

This concern has encouraged many organizations and researchers to propose several metrics to evaluate security of their information systems. In general, there is a consensus regarding the fact that choosing these metrics depends on the concrete security need of each organization. The majority of performed proposals put forward methods to choose these metrics [1, 4, 19, 22, 27, 28]. In addition, sometimes, it is suggested the need of developing specific methodologies for each organization [7].

In any proposal, the need is to quantify the different security aspects to be able to understand, control, and improve confidence in the information system.

If an organization does not use security metrics for its decision making process, the choices will be motivated by subjective aspects, external pressures and even purely commercial motivations.

With the purpose of systematizing all these proposals, we have developed a classification outline of security metrics [30] where the proposed metrics in the existing literature have been included. In our work, we will conclude that the majority of proposed metrics are general. This class of metrics only measure generic actions related to security and in an indirect way, specific objectives such as confidentiality, integrity and availability.

In this paper, we will propose metrics and indicators related to the password management policy due to the lack of specific proposals in special relevant areas in information system security.

In section 2, we will propose password management policy metrics justifying why they are necessary and classifying the proposed set according to several criteria. In section 3, we will put forward a classification according to levels of password management policies that allow organizations to know their current situation, to propose the relevant improvement and to relate comparisons between different institutions to know the best practices. Finally, we will present some of the obtained conclusions and a proposal of future work in this field.

## 2. Password Policy Metrics

We will propose a series of metrics that try to cover the most relevant factors of password management taken from the study performed about the problem of password management. These metrics do not try to cover the whole problem but to capture the most representative problems. In this hypothesis, it is not included the use of passwords for the authentication between processes or hosts. On the contrary, it is only studied the participation of a person as an entity to be authenticated. Multifactor authentication systems where one of the authentication mechanisms is a password are not included either.

The definition of these metrics will be performed by defining the following aspects:

- Name: Representative name of the metric.
- Description of the metric: Generally, it describes the name of the metric by indicating the method to calculate values.
- Life cycle phase: For a better understandability and analysis of measures, metrics are classified

according to their role within the life cycle of passwords.

The name and description of the metrics we have considered are as follows:

- *Users Training*: Type of training received by users for dealing with and selecting, if it is the case, passwords.
- *Group Password*: Existence of passwords used by a group of users or passwords necessary to access to resources that do not have an access control mechanism separated from the authentication mechanism.
- *Action Registers*: Type of register used by the information system to monitor the actions related to the password management.
- *Alphabet Size*: Number of characters of the alphabet used for the creation of passwords valid in the system.
- *Number of Different Classes Demanded*: Number of classes which the alphabet is divided into and that are required to determine a valid password.
- *Minimum Length*: Number of minimum characters required for a valid password.
- *Selection Source*: Set of agents that can be used to choose a password.
- *Selection Restriction*: Set of restrictions that avoid that the selection source uses a password easy to be found out by third parties.
- *User Identifier Class*: Type of user identifier used by the system.
- *Predefined Users*: Treatment that predefined users receive from the system.
- *Storage phase*: Way of passwords storage in the authentication system.
- *Initial Communication*: Method of communication of the initial password or a re-assignment of the user by the authentication system.
- *Net Transmission*: Mechanism of transmission used by the authentication protocol for the confidentiality and integrity of password.
- *Input Visualization*: Method used by the system for the visualization of the password when it is required to the user.
- *Maximum Number of Erroneous Attempts*: Maximum number of failed attempts before the authentication system makes a defense operation because of the risk of identity usurpation by a third party.
- *Information about Use*: Group of mechanisms used by the authentication system to inform the user about the authentications performed in the past.
- *Authentication Period*: Maximum time after which the access control asks for a user re-authentication.



- *Block by User Cancellation*: Procedures used to guarantee that users that were legitimate in the past, are avoided to access the system.
- *Minimum Life Time*: Minimum life time of a valid password.
- *Maximum Life Time*: Maximum life time of a valid password. When this time goes by, the user is forced to change the password.
- *Record Length*: Number of valid passwords used by the user in the past and that the system does not allow to reuse.
- *Password Reassigning*: Procedure used to reactivate the credential of a user that does not remember his password.

The proposed metrics are divided into a set of areas that correspond to the different phases of the life cycle of passwords in the system.

The areas we have considered are as follows (see Table 1 to analyze the area for each metric):

- *General*: Those metrics that could be in two or more areas are included.
- *Assignment*: All metrics related to the assigning of initial identifiers and passwords to the users are included.
- *Storage*: It contemplates the problem of storing passwords by the system.
- *Transmission*: It includes the metrics related to the authentication protocols used by the user or the communication of the password to the user by the authentication system.
- *Use*: Metrics that measure the way of use of the password by the user.
- *Renewal*: Area of metrics related to the password modification.

Metric	General	Assignment	Storage	Transmission	Use	Renewal
Users Training	√					
Group Password	√					
Action Register	√					
Alphabet Size		√				
Number of Different Classes Demanded		√				
Minimum Length		√				
Source Selection		√				
Selection Restriction		√				
User Identifier Class		√				
Predefined Users		√				
Storage Class			√			
Initial Communication				√		
Net Transmission				√		
Input Visualization					√	
Maximum Number of Erroneous Attempts					√	
Information about Use					√	
Authentication Period					√	
Block by User Cancellation						√
Minimum Life Time						√
Maximum Life Time						√
Record Length						√
Password Reassigning						√

Table 1. Classification of metrics according to areas

### 3. Security Levels

The definition of a set of metrics is not enough for an organization to be able to use them to manage the necessary changes in the field of those metrics. It is necessary to have information about the way of use and the impact of the values of the metrics on the system management.

With this objective, we have proposed some pre-established values for each metric that facilitates its use. Except for some of them, these values are ordered

according to a hierarchy, starting by a minimum value to a maximum one, passing through intermediate values in the majority of metrics. When an organization has a superior value in each metric, it will have a higher confidence in its authentication system.

As a general principle of computer security, it is not generally adequate to increase the values in some metrics without a generalized increase in all of them. Taking this principle as an objective, it is proposed an indicator of quality of password management policy based on five levels. This proposal is based on the

usefulness shown in the maturity models and in the metrics management programmes [5, 6, 8, 27].

These levels are structured from a minimum level (level 1) to a maximum level (level 5). The values required in each metric are defined in each level. In some of these metrics, it is also defined a recommended value for each level. These recommendations have the purpose of providing the indicator with flexibility, making it possible to define the required values at the lowest possible measure in each level.

When a metric has several values demanded in a level, this indicates that all those values should be had to consider that level has been reached. When in a metric it is demanded the same values in several levels, it is considered that the metric is in the higher level.

Anyway, the character of having recommended in a value of a metric does not have influence in its level and only has meaning for the calculation of the value of the indicator of quality of password management like it is described later on this section. Table 2 shows our analysis for each metric, considering the above-mentioned levels.

<b>Users Training</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
No Training	√				
Information when the user registration is made	Rec. <sup>1</sup>	√	√	√	√
Compulsory course	Rec.	Rec.	Rec.	√	√
Periodic course				Rec.	√
<b>Group Password</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Existence of group passwords or access to resources passwords	√				
Unique existence of a group of administrators		√	√		
There are not group passwords			Rec.	√	√
<b>Action Register</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
No action register	√				
Registration register		√	√	√	√
Renewal and cancellation register		Rec.	√	√	√
Block and re-assignment register		Rec.	Rec.	√	√
<b>Alphabet Size</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Less than or equal to ten characters	√				
Between eleven and twenty-five characters		√			
Between twenty-six and fifty characters		Rec.			
Between fifty-one and seventy-five characters			Rec.	√	
More than seventy-five characters			Rec.	Rec.	√
<b>Number of Different Classes demanded</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
One	√				
Two		√			
Three			√	√	
Four or more				Rec.	√
<b>Minimum Length</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Less than or equal to four characters	√				
Between five and eight characters		√			
Between nine and twelve characters			√		
Between thirteen and sixteen characters				√	
Greater than sixteen characters					√
<b>Source Selection</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
User	√	√	√	√	√
System				Rec.	Rec.
<b>Selection Restriction</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
No restriction					
User information	√	√	√	√	√
Keys combinations		Rec.	Rec.	√	√
Dictionary password			Rec.	√	√
Variations of the previous ones				Rec.	√
<b>User Identifier Class</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Public identifier	√	√	√		
Semi-public identifier			Rec.	√	
Private identifier				Rec.	√

<sup>1</sup> Rec.: Recommended

<b>Predefined Users</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
No change					
Password change	√	√	√	√	√
Identifier change			Rec.	√	√
<b>Storage Class</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Clear storage					
Irreversible storage	√	√	Rec.	Rec.	Rec.
Encrypted storage			√	√	√
<b>Initial Communication</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Non-secure transmission	√				
Transmission with compulsory change of password		√	√	Rec.	Rec.
Secure transmission			Rec.	√	√
<b>Net Transmission</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Clear transmission					
Use of a challenge-response protocol	√	√	√		
Encrypted transmission			Rec.	√	√
<b>Input Visualization</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Clear visualization					
Visualization of number of characters	√	√	√		
No visualization			Rec.	√	√
<b>Maximum Number of Erroneous Authentication Attempts</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
No limit	√				
Between eleven and fifty attempts	Rec.	√			
Between four and ten attempts		Rec.	√	√	
Less than or equal to three attempts				Rec.	√
<b>Information about Use</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
No information	√	√	√	√	√
Information about the last use			Rec.	Rec.	Rec.
<b>Authentication Period</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Work session	√	√			
Maximum of fifteen minutes inactivity			√	√	
Maximum of five minutes inactivity				Rec.	√
<b>Block by User Cancellation</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Without an established method	√				
Periodic elimination (maximum of six months period)	Rec.	√	√	√	√
Time limit established during registration			Rec.	√	√
<b>Minimum Life Time</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
There is not minimum life time	√	√	√	√	
There is a minimum life time (equal to or greater than 1 day)			Rec.	Rec.	√
<b>Maximum Life Time</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
Greater than twelve months	√				
Lower than or equal to twelve months		√			
Lower than or equal to six months			√	√	
Lower than or equal to three months				Rec.	√
<b>Record Length</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
One	√				
Lower than or equal to three		√			
Lower than or equal to ten			√		
Lower than or equal to twenty-five				√	
Greater than twenty-five					√
<b>Password Reassigning</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>
The previous password is reassigned	√				
A new password is assigned	Rec.	√	√	√	√

Table 2. Values according to the level of each metric.

The calculation of the value of the indicator of quality of the password management policy requires that the metrics values fulfil at least the "demanded"

requirement, and a minimum of values of these metrics must fulfil the recommended value too. The minimum

number of recommended values according to levels is shown in Table 3.

Level	Minimum number
1	3
2	3
3	8
4	7
5	2

**Table 3. Minimum number of metrics with recommended values**

### 3.1. Protection of Personal Data

The use of metrics and computer security indicators allow organizations to materialize their security objectives without a considerable effort. For example, in Spain, any organization from the public or the private sector must comply with the Real Decreto 994/1999 of 11th June that approves the regulation of security measures of the automated files containing personal data [24].

In this regulation, files are classified into three levels: basic, intermediate and high. Such levels are established according to the nature of the studied information, in relation to the higher or lower need to guarantee information confidentiality and integrity.

For low level files, article 11, in sections two and three, establishes that when the authentication mechanism is based on the existence of passwords, there will be an assignation, distribution and storage process that guarantee confidentiality and integrity. At the same time, passwords will be periodically changed according to the period of time established in the security document and, while they are valid they will be stored in a comprehensible way. Level 1 of our indicator of quality of password management policy widely fulfils these requirements.

Regarding intermediate level files, together with the security measures applicable to the low level files, complementary measures must be applied. Regarding identification and authentication, article 18 establishes that the person in charge of the file will establish a mechanism that allows the unequivocal identification of any user trying to access the information system and that the verification is authorized. In addition, the possibility of trying the non authorized access to the information system several times will be limited. In our case, Level 2 fulfils these requirements offering additional guarantees.

### 4. Conclusions and Future Work

The need to manage information systems security forces us to use metrics and indicators that allow us to

evaluate the real situation. In this work, we have proposed a set of metrics and password management policy indicators that fulfil this requirement in a practically generalized scope in any information system, the authentication process through passwords.

We have proposed twenty-two metrics grouped into six areas covering the whole cycle of password management. Due to the diversity of these metrics, where some of them have a potentially infinite value range (for instance, password length) and others have a very limited value range (for instance, password re-assignment), the definition of metrics includes a limited set of values that simplifies the process of obtaining measures and the use of metrics for decision making.

As a method of global valuation of the password management policy, it is proposed an indicator of quality whose range of values is formed by five levels. This indicator makes it possible to inform, in a single and comprehensible way, all actors involved in the organization security about the level of quality reached in an information system.

This proposal is made within the framework of a wider project of metrics definition that studies all security general areas. Nevertheless, in the area of identification and authentication, it is necessary to extend these metrics to the exploitation of the information system to complete the password management system.

Furthermore, the majority of organizations have a diversity of information systems with different requirements as well as different authentication mechanisms. To obtain an overall vision, through a set of metrics, it is necessary to combine all this information in a coherent and useful way for the organization board of directors and technical staff. In this aspect, the proposed metrics must be completed with others taking into account these circumstances.

Finally, we intend to be carried out like future works a study of the password management policy of a group of organizations selected to check the utility of the metric proposals, to validate the proposed group and to be a reference in best practices in this environment.

### 5. Acknowledgements

This research is part of the DIMENSIONS projects, partially financed by the FEDER and the Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), CALIPO (TIC2003-07804-C05-03) and RETISTIC (TIC2002-12487-E) granted by the "Dirección General de

Investigación del Ministerio de Ciencia y Tecnología” (Spain).

## 6. References

- [1] ACSA, editor. Proceedings of the Workshop on Information Security System Scoring and Ranking, Williamsburg, Virginia, may 2001.
- [2] A. Adams, M. A. Sasse, and P. Lunt. Making passwords secure and usable. In Proceedings of Human Computer Interaction, Bristol, England, aug 1997.
- [3] M. Bishop. Comparing authentication techniques. In Proceedings of the Third Workshop on Computer Incident Handling, pp. 1–10, aug 1991.
- [4] P. Bouvier and R. Longeon. Le tableau de bord de la sécurité du système d'information. *Sécurité Informatique*, jun 2003.
- [5] Carnegie Mellon University, Pittsburgh, Pennsylvania. SSE-CMM Model Description Document, 3.0 edition, jun 2003.
- [6] D. A. Chapin and S. Akridge. How can security be measured? *Information Systems Control Journal*, 2:43–47, 2005.
- [7] C. Colado and A. Franco. Métricas de seguridad: una visión actualizada. *SIC. Seguridad en Informática y Comunicaciones*, 57:64–66, nov 2003.
- [8] Department of the Air Force. AFI33-205. Information Protection Metrics and Measurements Program, aug 1997.
- [9] A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In Proceedings of the 14th International World Wide Web Conference, pp. 471–479, Chiba, Japan, may 2005.
- [10] ISO. ISO 7498-2. Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1989.
- [11] ISO/IEC. ISO/IEC TR 13335-1. Guidelines for the Management of IT Security. Part I: Concepts and Models of IT Security, 1996.
- [12] ISO/IEC. ISO/IEC 15408. Evaluation Criteria for IT Security, dec 1999.
- [13] ISO/IEC. ISO/IEC 17799. Code of Practice for Information Security Management, 2000.
- [14] G. King. Best security practices: An overview. In Proceedings of the 23rd National Information Systems Security Conference, Baltimore, Maryland, oct 2000. NIST.
- [15] J. M. Marcelo. Seguridad de las Tecnologías de la Información, capítulo Identificación y Evaluación de Entidades en un Método AGR, pp. 69–103. AENOR, 2003.
- [16] W. L. McKnight. What is information assurance? *CrossTalk. The Journal of Defense Software Engineering*, pp. 4–6, jul 2002.
- [17] R. T. Mercuri. Analyzing security costs. *CACM*, 46(6):15–18, jun 2003.
- [18] R. Morris and K. Thompson. Password security: A case history. *CACM*, 22(11):594–597, 1979.
- [19] F. Nielsen. Approaches of security metrics. Technical report, NIST-CSSPAB, jun 2000.
- [20] NIST. FIPS-112: Password Usage, may 1985.
- [21] NIST. FIPS-181: Automated Password Generator, oct 1993.
- [22] S. C. Payne. A guide to security metrics. Technical report, SANS Institute, jul 2001.
- [23] B. Pinkas and T. Sander. Securing passwords against dictionary attacks. In Proceedings of the ACM Computer and Security Conference (CSC' 02), pp. 161–170, nov 2002.
- [24] Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, jun 1999.
- [25] G. Schuedel and B. Wood. Adversary work factor as a metric for information assurance. In Proceedings of the New Security Paradigm Workshop, pp. 23–30, Ireland, sep 2000.
- [26] M. Swanson. Security self-assessment guide for information technology systems. Tech. Report NIST 800-26, National Institute of Standards and Technology, nov 2001.
- [27] M. Swanson, N. Bartol, J. Sabato, J. Hash, and L. Graffo. Security metrics guide for information technology systems. Technical Report NIST 800-55, National Institute of Standards and Technology, jul 2003.
- [28] R. B. Vaughn, Jr., R. Henning, and A. Siraj. Information assurance measures and metrics - state of practice and proposed taxonomy. In Proceedings of the 36th Hawaii International Conference on Systems Sciences, 2003.
- [29] R. B. Vaughn, Jr., A. Siraj, and D. A. Dampier. Information security system rating and ranking. *CrossTalk. The Journal of Defense Software Engineering*, pp. 30–32, may 2002.
- [30] C. Villarrubia, E. Fernández-Medina, and M. Piattini. Towards a classification of security metrics. In Proceedings of the 2nd international workshop on security in information systems (WOSIS 2004), pp. 342–350, apr 2004.