

The Third International Conference on Availability, Reliability and Security

(ARES 2008)

**Barcelona, Spain
4-7 March 2008**

Pages 1-760



IEEE Catalog Number: CFP0839A-PRT
ISBN: 978-1-4244-3049-9

TABLE OF CONTENTS

KEYNOTES

Security and Privacy Challenges in Location Based Service Environments.....	1
<i>Vijayalakshmi Atluri</i>	
Infrastructure support for Authorization, Access Control and Privilege Management.....	4
<i>Gunther Pernul</i>	
The ASCAA Principles for Next-Generation Role-Based Access Control	5
<i>Ravi Sandhu, Venkata Bhamidipati</i>	

ARES FULL PAPER SESSIONS

SESSION 1: APPLICATIONS

Securing Telehealth Applications in a Web-Based e-Health Portal.....	11
<i>Qian Liu, Shuo Lu, Yuan Hong, Lingyu Wang, Rachida Dssouli</i>	
Multi-Level Reputation-Based Greylisting	18
<i>Andreas G.K. Janecek, Wilfried N. Gansterer, K. Ashwin Kumar</i>	
Hardening XDS-Based Architectures.....	26
<i>Kim Wuyts, Riccardo Scandariato, Geert Claeys, Wouter Joosen</i>	

SESSION 2: MISCELLANEOUS

Finding Evidence of Antedating in Digital Investigations	34
<i>Svein Yngvar Willassen</i>	
FEDC: Control Flow Error Detection and Correction for Embedded Systems without Program Interruption	41
<i>Navid Farazmand, Mahdi Fazeli, Seyyed Ghasem Miremadi</i>	
Economic and Security Aspects of Applying a Threshold Scheme in e-Health	47
<i>Bernhard Riedl, Veronika Grascher, Mathias Kolb, Thomas Neubauer</i>	
Evaluation of Anomaly Based Character Distribution Models in the Detection of SQL Injection Attacks	55
<i>Mehdi Kiani, Andrew Clark, George Mohay</i>	
On the Possibility of Small, Service-Free Disk Based Storage Systems.....	64
<i>Jehan-François Pâris, Thomas J.E. Schwarz</i>	
Efficient High Availability Commit Processing.....	72
<i>Heine Kolltveit, Svein-Olaf Hvasshovd</i>	

SESSION 3: MODELS

Soundness Conditions for Message Encoding Abstractions in Formal Security Protocol Models	80
<i>Alfredo Pironti, Riccardo Sisto</i>	

Towards Formal Specification of Abstract Security Properties	88
<i>Antonio Maña, Gimena Pujol</i>	
A Behavioral Model of Ideologically-motivated “Snowball” Attacks.....	96
<i>Natalia Stakhanova, Oleg Stakhanov, Ali Ghorbani</i>	
Property Specification and Static Verification of UML Models	104
<i>Igor Siveroni, Andrea Zisman, George Spanoudakis</i>	

SESSION 4: DATABASE

Towards Comprehensive Requirement Analysis for Data Warehouses: Considering Security Requirements.....	112
<i>Emilio Soler, Veronika Stefanov, Jose-Norberto Mazon, Juan Trujillo, Eduardo Fernandez-Madina, Mario Piattini</i>	
A New Scheme for Distributed Density Estimation based Privacy-Preserving Clustering	120
<i>Chunhua Su, Feng Bao, Jianying Zhou, Tsuyoshi Takagi, Kouichi Sakurai</i>	
A Database Replication Protocol Where Multicast Writesets Are Always Committed	128
<i>Jose Ramon Juarez-Rodriguez, J.E. Armendariz-Iñigo, J.R. Gonzalez de Mendivil, F.D. Muñoz-Escoi</i>	

SESSION 5: MOBILE

Matching Policies with Security Claims of Mobile Applications	136
<i>Nataliia Bielova, Marco Dalla Torre, Nicola Dragoni, Ida Siahaan</i>	
PSecGCM: Process for the Development of Secure Grid Computing based Systems with Mobile Devices.....	144
<i>David G. Rosado, Eduardo Fernandez-Medina, Javier López, Mario Piattini</i>	
WATCHMAN: An Overlay Distributed AAA Architecture for Mobile Ad hoc Networks.....	152
<i>Amir R. Khakpour, Maryline Laurent-Maknavigius, Hakima Chaouchi</i>	

SESSION 6: RBAC AND RECOMMENDER

Hierarchical Domains for Decentralized Administration of Spatially-Aware RBAC Systems.....	161
<i>Maria Luisa Damiani, Claudio Silvestri, Elisa Bertino</i>	
Experimental Demonstration of a Hybrid Privacy-Preserving Recommender System	169
<i>Esma Aimeur, Gilles Brassard, Jose M. Fernandez, Flavien Serge Mani Onana, Zbigniew Rakowski</i>	
Fast Qualitative Reasoning about Actions for Computing Anticipatory Systems.....	179
<i>Natsumi Kitajima, Yuichi Goto, Jingde Cheng</i>	

SESSION 7: RISK MANAGEMENT

Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology	187
<i>Simon Tjoa, Stefan Jakoubi, Gerald Quirchmayr</i>	
Defining Secure Business Processes with Respect to Multiple Objectives.....	195
<i>Thomas Neubauer, Johannes Heurix</i>	
Analysis and Component-based Realization of Security Requirements.....	203
<i>Denis Hatebur, Maritta Heisel, Holger Schmidt</i>	

SESSION 8: NETWORKS

A Framework for Detecting Anomalies in VoIP Networks	212
<i>Yacine Bouzida, Christophe Mangin</i>	
Rapid Detection of Constant-Packet-Rate Flows	220
<i>Kuan-Ta Chen, Jing-Kai Lou</i>	
Performance Analysis of Anonymous Communication Channels Provided by Tor	229
<i>Andriy Panchenko, Lexi Pimenidis, Johannes Renner</i>	
Fast Algorithms for Consistency-Based Diagnosis of Firewall Rule Sets	237
<i>Sergio Pozo Hidalgo, Rafael Ceballos, Rafael Martínez Gasca</i>	
Privacy/Analysis Tradeoffs in Sharing Anonymized Packet Traces: Single-Field Case	245
<i>William Yurcik, Clay Woolam, Greg Hellings, Latifur Khan, Bhavani Thuraisingham</i>	
A Distributed Defense Framework for Flooding-Based DDoS Attacks	253
<i>Yonghua You, Mohammad Zulkernine, Anwar Haque</i>	
Pure MPLS Technology	261
<i>Liwen He, Paul Botham</i>	
Symmetric Active/Active Replication for Dependent Services	268
<i>Christian Engelmann, Stephen L. Scott, Chokchai Leangsuksun, Xubin He</i>	

SESSION 9: SOFTWARE

Statically Checking Confidentiality of Shared Memory Programs with Dynamic Labels	276
<i>Marcus Völz</i>	
A Cause-Based Approach to Preventing Software Vulnerabilities	284
<i>David Byers, Nahid Shahmehri</i>	
Integrating a Security Plug-in with the OpenUP/Basic Development Process	292
<i>Shanai Ardi, Nahid Shahmehri</i>	
A Novel Testbed for Detection of Malicious Software Functionality	300
<i>Jostein Jensen</i>	
Type and Effect Annotations for Safe Memory Access in C	310
<i>Syrine Tlili, Mourad Debbabi</i>	

SESSION 10: IDS AND MODELS

Adaptability of a GP Based IDS on Wireless Networks	318
<i>Adetokunbo Makanju, Nur Zincir-Heywood, Evangelos Milios</i>	
An Intrusion-Tolerant Mechanism for Intrusion Detection Systems	327
<i>Liwei Kuang, Mohammad Zulkernine</i>	
Fuzzy Private Matching (Extended Abstract)	335
<i>Lukasz Chmielewski, Jaap-Henk Hoepman</i>	

SESSION 11: TRUST, SECURITY AND ECONOMICS

Navigating in Webs of Trust: Finding Short Trust Chains in Unstructured Networks without Global Knowledge	343
<i>Jens-Uwe Bußer, Steffen Fries, Martin Otto, Peter Hartmann</i>	

Trust Modelling in E-Commerce through Fuzzy Cognitive Maps.....	352
<i>Christian Schläger, Günther Pernul</i>	
Boosting Markov Reward Models for Probabilistic Security Evaluation by Characterizing Behaviors of Attacker and Defender	360
<i>Zonghua Zhang, Farid Nait-Abdesselam, Pin-Han Ho</i>	

ARES SHORT PAPER SESSIONS

SESSION 1: APPLICATIONS

CERTILOC: Implementation of a Spatial-Temporal Certification Service Compatible with Several Localization Technologies	368
<i>José María de Fuentes García-Romero de Tejada, Ana Isabel González-Tablas Ferreres, Arturo Ribagorda Garnacho</i>	
Extending Mixed Serialisation Graphs to Replicated Environments	374
<i>Josep M. Bernabé-Gisbert, Francesc D. Muñoz-Escóí</i>	
Towards Secure E-Commerce Based on Virtualization and Attestation Techniques	381
<i>Frederic Stumpf, Claudia Eckert, Shane Balfe</i>	
Fuzzy Belief-Based Supervision	388
<i>Alexandre Vorobiev, Rudolph Seviara</i>	
Ensuring Progress in Amnesiac Replicated Systems.....	395
<i>Rubén de Juan-Marín, Luis Irún-Briz, Francesc D. Muñoz-Escóí</i>	
Enhancing Face Recognition with Location Information.....	402
<i>R.J. Hulsebosch, P.W.G. Ebben</i>	
A Lazy Monitoring Approach for Heartbeat-Style Failure Detectors.....	409
<i>Benjamin Satzger, Andreas Pietzowski, Wolfgang Trumler, Theo Ungerer</i>	
Defending On-Line Web Application Security with User-Behavior Surveillance.....	415
<i>Yu-Chin Cheng, Chi-Sung Lai, Gu-Hsin Lai, Chia-Mei Chen, Tsuhan Chen</i>	

SESSION 2: SERVICES AND TRUST

A Pattern-Driven Security Process for SOA Applications	421
<i>Nelly A. Delessy, Eduardo B. Fernandez</i>	
Towards a Dependable Architecture for Highly Available Internet Services.....	427
<i>Pablo Neira Ayuso, Laurent Lefèvre, Denis Barbaron, Rafael M. Gasca</i>	
Assessing the Reliability and Cost of Web and Grid Orchestrations	433
<i>Alan Stewart, Maurice Clint, Terry Harmer, Peter Kilpatrick, Ron Perrott, Joaquim Gabarro</i>	
Application-Oriented Trust in Distributed Computing.....	439
<i>Riccardo Scandariato, Yoram Ofek, Paolo Falcarin, Mario Baldi</i>	
BlueTrust in a Real World	445
<i>Bradley Markides, Marijke Coetzee</i>	

SESSION 3: PRIVACY AND SAFETY

Privacy Preserving Shortest Path Computation in Presence of Convex Polygonal Obstacles	451
<i>Ananda Swarup Das, Jitu Kumar Keshri, Kannan Srinathan, Vaibhav Srivastava</i>	

Privacy Protected ELF for Private Computing on Public Platforms	457
<i>Thomas H. Morris, V.S.S. Nair</i>	
haplog: A Hash-Only and Privacy-Preserved Secure Logging Mechanism	463
<i>Chih-Yin Lin</i>	
An Improved Zonal Safety Analysis Method and Its Application on Aircraft CRJ200	466
<i>Li Xiaolei, Tian Jin, Zhao Tingdi</i>	

SESSION 4: NETWORKS

A Model for Specification and Validation of Security Policies in Communication Networks: The Firewall Case	472
<i>Ryma Abbassi, Sihem Guemara El Fatmi</i>	
SPIT Detection and Prevention Method in VoIP Environment	478
<i>He Guang-Yu, Wen Ying-You, Zhao Hong</i>	
A New Approach to Analysis of Interval Availability	484
<i>Ezzat Kirmani, Cynthia S. Hood</i>	
SFMD: A Secure Data Forwarding and Malicious Routers Detecting Protocol	489
<i>Xiang-he Yang, Hua-ping Hu, Xin Chen</i>	
Fault Effects in FlexRay-Based Networks with Hybrid Topology	496
<i>Mehdi Dehbashi, Vahid Lari, Seyed Ghassem Miremadi, Mohammad Shokrollah-Shirazi</i>	
Secure Wireless Sensor Networks	502
<i>Xun Yi, Mike Faulkner, Eiji Okamoto</i>	
SEIF: Secure and Efficient Intrusion-Fault Tolerant Routing Protocol for Wireless Sensor Networks	508
<i>Abdelraouf Ouadjaout, Yacine Challal, Nouredine Lasla, Miloud Bagaa</i>	
The Impact of Flooding Attacks on Network-based Services	514
<i>Meiko Jensen, Nils Gruschka, Norbert Luttenberger</i>	
Managing Priorities in Atomic Multicast Protocols	519
<i>Emili Miedes, Francesc D. Muñoz-Escóí</i>	
Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks	525
<i>Asier Martínez, Urko Zurutuza, Roberto Uribeetxeberria, Miguel Fernández, Jesus Lizarraga, Ainhoa Serna, Iñaki Vélez</i>	
An End-to-End Security Solution for SCTP	531
<i>Stefan Lindskog, Anna Brunstrom</i>	

SESSION 5: CRYPTO

An Identity-Based Group Key Agreement Protocol from Pairing	537
<i>Hongji Wang, Gang Yao, Qingshan Jiang</i>	
An Authenticated 3-Round Identity-Based Group Key Agreement Protocol	543
<i>Gang Yao, Hongji Wang, Qingshan Jiang</i>	
High Capacity Steganographic Method Based Upon JPEG	549
<i>Adel Almohammad, Robert M. Hierons, Gheorghita Ghinea</i>	
Cluster-based Group Key Agreement for Wireless Ad hoc Networks	555
<i>Elisavet Konstantinou</i>	

SESSION 6: CRYPTO AND HEALTH

A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words	563
<i>Chen Zhi-li, Huang Liu-sheng, Yu Zhen-shan, Li Ling-jun, Yang Wei</i>	
RTQG: Real-Time Quorum-based Gossip Protocol for Unreliable Networks	569
<i>Bo Zhang, Kai Han, Binoy Ravindran, E.D. Jensen</i>	
A Secure and Scalable Infrastructure for Inter-Organizational Data Exchange and eGovernment Applications	577
<i>Jan Willemson, Arne Ansper</i>	
A Security Model and its Application to a Distributed Decision Support System for Healthcare	583
<i>Liang Xiao, Javier Vicente, Carlos Sáez, Andrew Peet, Alex Gibb, Paul Lewis, Srinandan Dasmahapatra, Madalina Croitoru, Horacio González-Vélez, Magí Lluch i Ariet, David Dupplaw</i>	

SESSION 7: MODELS AND NETWORKS

Run-time Information Flow Monitoring based on Dynamic Dependence Graphs.....	591
<i>Salvador Cavadini, Diego Cheda</i>	
Automated Process Classification Framework using SELinux Security Context.....	597
<i>Pravin Shinde, Priyanka Sharma, Srinivas Guntupalli</i>	
Using Composition Policies to Manage Authentication and Authorization Patterns and Services.....	602
<i>Judith E.Y. Rossebø, Rolv Bræk</i>	
Providing Fault Tolerance in Wireless Backhaul Network Design with Path Restoration	609
<i>Narueemon Wattanapongsakorn, Chalermpol Charnsripinyo, Pakorn Leesutthipornchai</i>	

SESSION 8: IDS

Histogram Matrix: Log File Visualization for Anomaly Detection	615
<i>Adrian Frei, Marc Rennhard</i>	
Context-based Profiling for Anomaly Intrusion Detection with Diagnosis.....	623
<i>Benferhat Salem, Tabia Karim</i>	
A Revised Taxonomy of Data Collection Mechanisms with a Focus on Intrusion Detection	629
<i>Ulf Larson, Erland Jonsson, Stefan Lindskog</i>	
IDRS: Combining File-level Intrusion Detection with Block-level Data Recovery based on iSCSI.....	635
<i>Youhui Zhang, Hongyi Wang, Yu Gu, Dongsheng Wang</i>	
Intrusion Detection for Wormhole Attacks in Ad hoc Networks: A Survey and a Proposed Decentralized Scheme	641
<i>Marianne Azer, Sherif El-Kassas, Abdel Wahab Hassan, Magdy El-Soudani</i>	

SESSION 9: HARDWARE

NFC Devices: Security and Privacy	647
<i>Gerald Madlmayr, Josef Langer, Christian Kantner, Josef Scharinger</i>	
Analyzing Fault Effects in the 32-bit OpenRISC 1200 Microprocessor	653
<i>Nima Mehdizadeh, Mohammad Shokrolah-Shirazi, Seyed Ghassem Miremadi</i>	

Increasing the Performability of Computer Clusters Using RADIC II	658
<i>Guna Santos, Angelo Duarte, Dolores, Emilio Luque</i>	
A Framework for Proactive Fault Tolerance	664
<i>Geoffroy Vallee, Kulathep Charoenpornwattana, Christian Engelmann, Anand Tikotekar, Chokchai Leangsuksun, Thomas Naughton, Stephen L. Scott</i>	

WORKSHOP FARES

SESSION 1: MISCELLANEOUS

Anti-DDoS Virtualized Operating System	670
<i>Sanjam Garg, Huzur Saran</i>	
A Case for High Availability in a Virtualized Environment (HAVEN)	678
<i>Erin Farr, Richard Harper, Lisa Spainhower, Jimi Xenidis</i>	

SESSION 2: ACCESS CONTROL AND ALGORITHMS

A Federated Physical and Logical Access Control Enforcement Model	686
<i>Stéphane Onno</i>	
Fostering the Uptake of Secure Multiparty Computation in E-Commerce	696
<i>Octavian Catrina, Florian Kerschbaum</i>	
Efficient Certificate Path Validation and Its Application in Mobile Payment Protocols	704
<i>Rafael Martinez-Peláez, Cristina Satizábal, Francisco Rico-Novella, Jordi Forné</i>	
Avoiding Policy-based Deadlocks in Business Processes	712
<i>Mathias Kohler, Andreas Schaad</i>	
A Secure High-Speed Identification Scheme for RFID Using Bloom Filters	720
<i>Yasunobu Nohara, Sozo Inoue, Hiroto Yasuura</i>	

SESSION 3: CRYPTO

New Self Certified Proxy Digital Signature Scheme based on Elliptic Curve Cryptosystem	726
<i>Youan Xiao</i>	
Privacy-preserving Protocols for Finding the Convex Hulls	730
<i>Qi Wang, Yonglong Luo, Liusheng Huang</i>	
A Secure RFID Protocol based on Insubvertible Encryption Using Guardian Proxy	736
<i>Kyosuke Osaka, Shuang Chang, Tsuyoshi Takagi, Kenichi Yamazaki, Osamu Takahashi</i>	
Cryptographic Properties of Second-Order Memory Elementary Cellular Automata	744
<i>Ascension Hernández Encinas, Angel Martín del Rey, J.L. Pérez Iglesias, Gerardo Rodríguez Sánchez, Araceli Queiruga Dios</i>	
New Efficient and Authenticated Key Agreement Protocol in Dynamic Peer Group	749
<i>Shengke Zeng, Mingxing He, Weidong Luo</i>	

SESSION 4: RISK MANAGEMENT

Intensive Programme on Information and Communication Security	755
<i>Christian Schläger, Ludwig Fuchs, Günther Pernul</i>	
Applications for IT-Risk Management – Requirements and Practical Evaluation	761
<i>Heinz Lothar Grob, Gereon Strauch, Christian Buddendick</i>	

Security Analysis of Role-based Separation of Duty with Workflows.....	768
<i>Rattikorn Hewett, Phongphun Kijsanayothin, Aashay Thipse</i>	

SESSION 5: DATABASES AND MODELS

Detecting Suspicious Relational Database Queries	774
<i>Stefan Böttcher, Rita Hartel, Matthias Kirschner</i>	
Assessing the Value of Enterprise Identity Management (EIdM) – Towards a Generic Evaluation Approach	782
<i>Denis Royer</i>	
An Ontological Approach to Secure MANET Management	790
<i>Mark E. Orwat, Timothy E. Levin, Cynthia E. Irvine</i>	

SESSION 6: MODELS

Reliability Analysis using Graphical Duration Models.....	798
<i>Roland Donat, Laurent Bouillaut, Patrice Aknin, Philippe Leray</i>	
From Omega to $\Diamond$P in the Crash-Recovery Failure Model with Unknown Membership	804
<i>Mikel Larrea, Cristian Martín</i>	
Policy-based Group Organizational Structure Management using an Ontological Approach.....	810
<i>Mario Anzures-García, Luz A. Sánchez-Gálvez</i>	
A Systematic Review and Comparison of Security Ontologies	816
<i>Carlos Blanco, Joaquín Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, Mario Piattini</i>	
Context Ontology for Secure Interoperability	824
<i>Céline Coma, Nora Cuppens-Boulahia, Frédéric Cuppens, Ana-Rosa Cavalli</i>	

SESSION 7: PASSWORDS AND SERVICES

On the Security of VSH in Password Schemes	831
<i>Kimmo Halunen, Pauli Rikula, Juha Rönning</i>	
Sustaining Web Services High-Availability Using Communities.....	837
<i>Zakaria Maamar, Quan Z. Sheng, Djamal Benslimane</i>	
Distributed Information Retrieval Service for Ubiquitous Services.....	845
<i>Takeshi Tsuchiya, Marc Lihan, Hirokazu Yoshinaga, Keiichi Koyanagi</i>	

SESSION 8: SOFTWARE

A Lightweight Security Analyzer inside GCC	854
<i>Davide Pozza, Riccardo Sisto</i>	
Dynamic Maintenance of Software Systems at Runtime	862
<i>Habib Seifzadeh, Mostafa Kermani, Mohsen Sadighi</i>	
Software Security; A Vulnerability Activity Revisit	869
<i>Mohammad Ali Hadavi, Hossein Shirazi, Hasan Mokhtari Sangchi, Vahid Saber Hamishagi</i>	

SESSION 9: TRUST

Making Multi-Dimensional Trust Decisions on Inter-Enterprise Collaborations.....	876
<i>Sini Ruohomaa, Lea Kutvonen</i>	

A Survey on Trust and Reputation Schemes in Ad Hoc Networks.....	884
<i>Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F. Hassan, Magdy S. El-Soudani</i>	

WORKSHOP WPA

Privacy-Preserving Recommendation Systems for Consumer Healthcare Services	890
<i>Stefan Katzenbeisser, Milan Petkovic</i>	

Detecting Bots Based on Keylogging Activities.....	897
<i>Yousof Al-Hammadi, Uwe Aickelin</i>	

A Comprehensive Approach for Context-dependent Privacy Management.....	904
<i>Elke Franz, Christin Groba, Thomas Springer, Mike Bergmann</i>	

Traceable Quantitative Risk Assessment Applied to Investment Decision for Local Backups	912
<i>Steffen Weiss, Martin Wahl, Michael Tielemann, Klaus Meyer-Wegener</i>	

Quantitative Assessment of Enterprise Security System	922
<i>Ruth Breu, Frank Innerhofer-Oberperfler, Artsiom Yautsiukhin</i>	

Clustering Oriented Architectures in Medical Sensor Environments.....	930
<i>Eleni Klaoudatou, Elisavet Konstantinou, Georgios Kambourakis, Stefanos Gritzalis</i>	

An Initial Model and a Discussion of Access Control in Patient Controlled Health Records	936
<i>Lillian Røstad</i>	

Secure Team-Based EPR Access Acquisition in Wireless Networks	944
<i>Sigurd Eskeland, Vladimir Oleshchuk</i>	

VEA-bility Security Metric: A Network Security Analysis Tool	951
<i>Melanie Tupper, A. Nur Zincir-Heywood</i>	

Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments	959
<i>Stefan G. Weber, Andreas Heinemann, Max Mühlhäuser</i>	

WORKSHOP PSAI

GOST-28147 Encryption Implementation on Graphics Processing Units	966
<i>Victor Korobitsin, Sergey Ilyin</i>	

Intelligent Video Surveillance Networks: Data Protection Challenges	974
<i>Fanny Coudert, Jos Dumortier</i>	

Intrusion Detection with Data Correlation Relation Graph.....	981
<i>Amin Hassanzadeh, Babak Sadeghian</i>	

A Critique of k-Anonymity and Some of Its Enhancements	989
<i>Josep Domingo-Ferrer, Vicenç Torra</i>	

Cluster-Specific Information Loss Measures in Data Privacy: A Review.....	993
<i>Vicenç Torra, Susana Ladra</i>	

Hierarchical Trust Architecture in a Mobile Ad-Hoc Network Using Ant Algorithms.....	999
<i>Cristina Satizábal, Jordi Forné, Rafael Martínez-Peláez, Franciso Rico-Novella</i>	

Representation and Reasoning on ORBAC: Description Logic with Defaults and Exceptions Approach	1007
<i>Narhimene Boustia, Aicha Mokhtari</i>	
Using Non-adaptive Group Testing to Construct Spy Agent Routes.....	1012
<i>Georgios Kalogridis, Chris J. Mitchell</i>	
A Bayesian Approach for on-Line Max Auditing	1019
<i>Gerardo Canfora, Bice Cavallo</i>	
Detection of Malcodes by Packet Classification.....	1027
<i>Irfan Ahmed, Kyung-suk Lhee</i>	
Performance of a Strategy Based Packets Forwarding in Ad Hoc Networks	1035
<i>Marcin Seredynski, Pascal Bouvry, Mieczyslaw A. Klopotek</i>	
Bayesian Additive Regression Trees-Based Spam Detection for Enhanced Email Privacy	1043
<i>Saeed Abu-Nimeh, Dario Nappa, Xinlei Wang, Suku Nair</i>	
AntTrust: A Novel Ant Routing Protocol for Wireless Ad-hoc Network Based on Trust between Nodes	1051
<i>Carlos Aguilar Melchor, Boussad Ait Salem, Philippe Gaborit, Karim Tamine</i>	
A Post-processing Method to Lessen k-Anonymity Dissimilarities.....	1059
<i>Agusti Solanas, Gloria Pujol, Antoni Martinez-Balleste, Josep M. Mateo-Sanz</i>	
Improving Techniques for Proving Undecidability of Checking Cryptographic Protocols	1066
<i>Zhiyao Liang, Rakesh M Verma</i>	
A Preliminary Investigation of Skype Traffic Classification Using a Minimalist Feature Set	1074
<i>Duffy Angevine, Nur Zincir-Heywood</i>	

WORKSHOP APE

Partial Disclosure of Searchable Encrypted Data with Support for Boolean Queries.....	1079
<i>Yasuhiro Ohtaki</i>	
Secure and Privacy-Friendly Logging for eGovernment Services.....	1087
<i>Karel Wouters, Koen Simoens, Danny Lathouwers, Bart Preneel</i>	
The REM Framework for Security Evaluation	1093
<i>Flora Amato, Valentina Casola, Antonino Mazzeo, Valeria Vittorini</i>	
Static Validation of Licence Conformance Policies.....	1100
<i>Rene Rydhof Hansen, Flemming Nielson, Hanne Riis Nielson, Christian W. Probst</i>	
Towards Practical Security Monitors of UML Policies for Mobile Applications	1108
<i>Fabio Massacci, Katsiaryna Naliuka</i>	
Synthesis of Local Controller Programs for Enforcing Global Security Properties	1116
<i>Fabio Martinelli, Ilaria Matteucci</i>	
Weighted Datalog and Levels of Trust	1124
<i>Stefamno Bistarelli, Fabio Martinelli, Francesco Santini</i>	
Negotiation of Usage Control Policies - Simply the Best?.....	1131
<i>Alexander Pretschner, Thomas Walter</i>	

WORKSHOP SECSE

Security Requirement Engineering at a Telecom Provider	1133
<i>Albin Zuccato, Viktor Endersz, Nils Daniels</i>	

Identifying Security Aspects in Early Development Stages	1142
<i>Takao Okubo, Hidehiko Tanaka</i>	
Using Security Patterns to Combine Security Metrics	1150
<i>Thomas Heyman, Riccardo Scandariato, Christophe Huygens, Wouter Joosen</i>	
Secure Software Design in Practice	1158
<i>Per Håkon Meland, Jostein Jensen</i>	
Covering Your Assets in Software Engineering	1166
<i>Martin Gilje Jaatun, Inger Anne Tøndel</i>	
A Non-Intrusive Approach to Enhance Legacy Embedded Control Systems with Cyber Protection Features	1174
<i>Shangping Ren, Kevin Kwiat</i>	
Towards Incorporating Discrete-Event Systems in Secure Software Development	1182
<i>Sarah Whittaker, Mohammad Zulkernine, Karen Rudie</i>	
How to Open a File and Not Get Hacked	1190
<i>James A. Kupsch, Barton P. Miller</i>	
Rules of Thumb for Developing Secure Software: Analyzing and Consolidating Two Proposed Sets of Rules	1198
<i>Holger Peine</i>	

WORKSHOP DAWAM

Adaptive Data Integrity through Dynamically Redundant Data Structures	1204
<i>Vincenzo De Florio, Chris Blondia</i>	
ISEDS: An Information Security Engineering Database System Based on ISO Standards	1210
<i>Daisuke Horie, Shoichi Morimoto, Noor Azimah, Yuichi Goto, Jingde Cheng</i>	
Privacy Aspects of eHealth	1217
<i>Daniel Slamanig, Christian Stingl</i>	
Adaptive Voting Algorithms for Reliable Dissemination of Data in Sensor Networks	1225
<i>Kaliappa Ravindran, Jiang Wu, Kevin A. Kwiat, Ali Sabbir</i>	
Risk as Dependability Metrics for the Evaluation of Business Solutions: A Model-driven Approach	1231
<i>Yudistira Asnar, Rocco Moretti, Maurizio Sebastianis, Nicola Zannone</i>	
Implementing Multidimensional Security into OLAP Tools	1239
<i>Carlos Blanco, Eduardo Fernández-Medina, Juan Trujillo, Mario Piattini</i>	
Detecting Key Players in 11-M Terrorist Network: A Case Study	1245
<i>Nasrullah Memon, David L. Hicks</i>	
Privacy Preserving Support Vector Machines in Wireless Sensor Networks	1251
<i>Dong Seong Kim, Muhammad Anwarul Azim, Jong Sou Park</i>	
An Image Encryption System by Cellular Automata with Memory	1257
<i>Farhad Maleki, Ali Mohades, S. Mehdi Hashemi, Mohammad Ebrahim Shiri</i>	

WORKSHOP WAIS

Insider-secure Signcryption KEM/Tag-KEM Schemes without Random Oracles	1263
<i>Chik How Tan</i>	

Internet Observation with ISDAS: How Long Does a Worm Perform Scanning?	1270
<i>Tomohiro Kobori, Hiroaki Kikuchi, Masato Terada</i>	
Electronic Voting Scheme to Maintain Anonymity in Small-scale Election by Hiding the Number of Votes.....	1275
<i>Tsukasa Endo, Isao Echizen, Hiroshi Yoshiura</i>	
Enocoro-80: A Hardware Oriented Stream Cipher	1282
<i>Dai Watanabe, Kota Ideguchi, Jun Kitahara, Kenichiro Muto, Hiroki Furuichi, Toshinobu Kaneko</i>	
Cryptanalysis and Improvement of an ‘Improved Remote Authentication Scheme with Smart Card’	1289
<i>Marko Hölbl, Tatjana Welzer</i>	
Effective Monitoring of a Survivable Distributed Networked Information System.....	1294
<i>Paul Rubel, Michael Atighetchi, Partha Pal, Martin Fong, Richard O'Brien</i>	
Design of an FDB based Intra-domain Packet Traceback System	1301
<i>Hiroaki Hazeyama, Yoshihide Matsumoto, Youki Kadobayashi</i>	
An Independent Evaluation of Web Timing Attack and its Countermeasure.....	1307
<i>Yoshitaka Nagami, Daisuke Miyamoto, Hiroaki Hazeyama, Youki Kadobayashi</i>	
Secure Spatial Authentication for Mobile Stations In Hybrid 3G-WLAN Serving Networks	1313
<i>Arjan Durresi, Mimoza Durresi, Leonard Barolli</i>	
Privacy-Preserving Distributed Set Intersection	1320
<i>Qingsong Ye, Huaxiong Wang, Christophe Tartary</i>	
Examination of Forwarding Obstruction Attacks in Structured Overlay Networks.....	1328
<i>Yo Mashimo, Shintaro Ueda, Yasutaka Shinzaki, Hiroshi Shigeno</i>	
A Novel Approach for Multiplication over GF(2m) in Polynomial Basis Representation.....	1334
<i>Abdulah Abdulah Zadeh</i>	

WORKSHOP WSDF

Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics.....	1340
<i>Benjamin Turnbull, Jill Slay</i>	
Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis.....	1346
<i>Joshua Broadway, Benjamin Turnbull, Jill Slay</i>	
Recovery of Encryption Keys from Memory Using a Linear Scan.....	1354
<i>Christopher Hargreaves, Howard Chivers</i>	
Proposal for Efficient Searching and Presentation in Digital Forensics	1362
<i>Jooyoung Lee</i>	
Secure Steganography in Compressed Video Bitstreams	1367
<i>Bin Liu, Fenlin Liu, Chunfang Yang, Yifeng Sun</i>	
Considerations Towards a Cyber Crime Profiling System.....	1373
<i>Kweku K. Arthur, Martin S. Olivier, Hein S. Venter, Jan H.P. Eloff</i>	

WORKSHOP SREIS

Alignment of Misuse Cases with Security Risk Management	1379
<i>Raimundas Matulevicius, Nicolas Mayer, Patrick Heymans</i>	

Information Stream Based Model for Organizing Security	1387
<i>Bernhard Thalheim, Sabah Al-Fedaghi, Khaled Al-Saqabi</i>	
Security Requirements Variability for Software Product Lines	1395
<i>Daniel Mellado, Eduardo Fernandez-Medina, Mario Piattini</i>	
Transforming Security Requirements into Architecture.....	1403
<i>Koen Yskout, Riccardo Scandariato, Bart De Win, Wouter Joosen</i>	
Modelling Security Properties in a Grid-based Operating System with Anti-Goals.....	1411
<i>Alvaro Arenas, Benjamin Aziz, Juan Bicarregui, Brian Matthews, Erica Y. Yang</i>	
Annotating Regulations Using Cerno: An Application to Italian Documents - Extended Abstract.....	1419
<i>Nicola Zeni, Nadzeya Kiyavitskaya, James R. Cordy, Luisa Mich, John Mylopoulos</i>	
Goal-Oriented, B-Based Formal Derivation of Security Design Specifications from Security Requirements.....	1425
<i>Riham Hassan, Shawn Bohner, Sherif El-Kassas, Mohamed Eltoweissy</i>	
Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract)	1433
<i>Orhan Cetinkaya</i>	
Author Index	