

2009 International Conference on Availability, Reliability, and Security

(ARES)

**Fukuoka, Japan
16 – 19 March 2009**

Pages 1-480



**IEEE Catalog Number: CFP0939A-PRT
ISBN: 978-1-4244-3572-2**

2009 International Conference on Availability, Reliability and Security

ARES 2009

Table of Contents

Message from General Co-chairs
Message from ARES Workshops' Co-chairs
Conference Officers
Program Committee
Message from DAWAM Workshop Co-chairs
DAWAM Organization Co-chairs
DAWAM Program Committee
DAWAM Reviewers
Message from FARES Workshop Co-chairs
FARES Organization Committee
FARES Program Committee
FARES Reviewers
Message from GloSec Workshop Chair
GloSec Organization Committee
GloSec Program Committee
GloSec Reviewers
Message from IWSS Workshop Co-chairs
IWSS Organization Committee
IWSS Program Committee
IWSS Reviewers
Message from OSA Workshop Co-chairs
OSA Organization Committee
OSA Program Committee
OSA Reviewers
Message from RIBC Workshop Co-chairs
RIBC Organization Committee
RIBC Program Committee
RIBC Reviewers
Message from SecSE Workshop Co-chairs
SecSE Organization Committee

SecSE Program Committee
SecSE Reviewers
Message from SECUSAB Workshop Co-chairs
SECUSAB Organization Committee
SECUSAB Program Committee
SECUSAB Reviewers
Message from WAIS Workshop Co-chairs
WAIS Organization Committee
WAIS Program Committee
WAIS Reviewers
Message from WSDF Workshop Co-chairs
WSDF Organization Committee
WSDF Program Committee
WSDF Reviewers
**Keynote 1: Pairing Based Cryptography - Theory, Implementations
and Applications**
Keynote 2: Digital Identity Protection - Concepts and Issues
Keynote 3: Topological Analysis of Network Attack Vulnerability
**Invited Talk: Integrative Security Approach as a Key Success Factor
of Dependability**

Distributed Systems and Grid (ARES Full Papers)

A Pluggable Domain Management Approach for Building Practical Distributed Coalitions	1
<i>Yasuharu Katsuno, Yuji Watanabe, Michiharu Kudo, and Eiji Okamoto</i>	
Retaining Data Control to the Client in Infrastructure Clouds	9
<i>Marco Descher, Philip Masser, Thomas Feilhauer, A. Min Tjoa, and David Huemer</i>	
Workflows in Dynamic and Restricted Delegation	17
<i>Mehran Ahsant and Jim Basney</i>	

SOA Security (ARES Full Papers)

The Accountability Problem of Flooding Attacks in Service-Oriented Architectures	25
<i>Meiko Jensen and Jörg Schwenk</i>	
Web Service Trust: Towards a Dynamic Assessment Framework	33
<i>George Spanoudakis and Stephane LoPresti</i>	
Security Requirements Specification in Service-Oriented Business Process Management	41
<i>Michael Menzel, Ivonne Thomas, and Christoph Meinel</i>	

Enterprise Security 1 (ARES Full Papers)

Quantitative Analysis of Secure Information Flow via Probabilistic Semantics	49
<i>Chunyan Mu and David Clark</i>	
Deploying Security Policy in Intra and Inter Workflow Management Systems	58
<i>Samiha Ayed, Nora Cuppens-Boulahia, and Frédéric Cuppens</i>	
An Empirically Derived Loss Taxonomy Based on Publicly Known Security Incidents	66
<i>Frank Innerhofer-Oberperfler and Ruth Breu</i>	

Intrusion and Fraud Detection (ARES Full Papers)

Defeating Dynamic Data Kernel Rootkit Attacks via VMM-Based Guest-Transparent Monitoring	74
<i>Junghwan Rhee, Ryan Riley, Dongyan Xu, and Xuxian Jiang</i>	
Server-Side Prediction of Source IP Addresses Using Density Estimation	82
<i>Markus Goldstein, Matthias Reif, Armin Stahl, and Thomas Breuel</i>	
Detecting Stepping-Stone Connection Using Association Rule Mining	90
<i>Ying-wei Kuo and Shou-Hsuan Stephen Huang</i>	

Enterprise Security 2 (ARES Full Papers)

Formal Analyses of Usage Control Policies	98
<i>Alexander Pretschner, Judith Rüesch, Christian Schaefer, and Thomas Walter</i>	
A First Step towards Characterizing Stealthy Botnets	106
<i>Justin Leonard, Shouhuai Xu, and Ravi Sandhu</i>	
Intrusion Process Modeling for Security Quantification	114
<i>Jaafar Almasizadeh and Mohammad Abdollahi Azgomi</i>	
Different Approaches to In-House Identity Management - Justification of an Assumption	122
<i>L. Fuchs, C. Broser, and G. Pernul</i>	

Digital Forensics and Security in Communication (ARES Full Papers)

An LPN-Problem-Based Lightweight Authentication Protocol for Wireless Communications	130
<i>Ya-Fen Chang and Yen-Cheng Lai</i>	
Revealing the Calling History of SIP VoIP Systems by Timing Attacks	135
<i>Ge Zhang, Simone Fischer-Huebner, Leonardo A. Martucci, and Sven Ehlert</i>	
The Anatomy of Electronic Evidence – Quantitative Analysis of Police E-Crime Data	143
<i>Benjamin Turnbull, Robert Taylor, and Barry Blundell</i>	
A Robust Image Watermarking Using Two Level DCT and Wavelet Packets Denoising	150
<i>A.H. Taherinia and M. Jamzad</i>	

Availability and Reliability 1 (ARES Full Papers)

On Equilibrium Distribution Properties in Software Reliability Modeling	158
<i>Xiao Xiao and Tadashi Dohi</i>	
An Analysis of Fault Effects and Propagations in AVR Microcontroller ATmega103(L)	166
<i>Alireza Rohani and Hamid. R. Zarandi</i>	
Blue Gene/L Log Analysis and Time to Interrupt Estimation	173
<i>Narate Taerat, Nichamon Naksinehaboon, Clayton Chandler, James Elliott, Chokchai Leangsuksun, George Ostrouchov, Stephen L. Scott, and Christian Engelmann</i>	

Cryptography (ARES Full Papers)

A New Approach for Implementing the MPL Method toward Higher SPA Resistance	181
<i>Masami Izumi, Kazuo Sakiyama, and Kazuo Ohta</i>	
On Privacy Preserving Convex Hull	187
<i>Sandeep Hans, Sarat C. Addepalli, Anuj Gupta, and Kannan Srinathan</i>	
Routing Protocol Security Using Symmetric Key Based Techniques	193
<i>Bezawada Bruhadeshwar, Kishore Kothapalli, M. Poornima, and M. Divya</i>	

Software Security 1 (ARES Full Papers)

Prioritisation and Selection of Software Security Activities	201
<i>David Byers and Nahid Shahmehri</i>	
BRICK: A Binary Tool for Run-Time Detecting and Locating Integer-Based Vulnerability	208
<i>Ping Chen, Yi Wang, Zhi Xin, Bing Mao, and Li Xie</i>	
Enhancing Automated Detection of Vulnerabilities in Java Components	216
<i>Pierre Parrend</i>	

Software Security 2 (ARES Full Papers)

Automated Support for Security Requirements Engineering in Software Product Line Domain Engineering	224
<i>Daniel Mellado, Jesus Rodríguez, Eduardo Fernández-Medina, and Mario Piattini</i>	
Identifying and Resolving Least Privilege Violations in Software Architectures	232
<i>Koen Buyens, Bart De Win, and Wouter Joosen</i>	
A Test Framework for Assessing Effectiveness of the Data Privacy Policy's Implementation into Relational Databases	240
<i>Gerardo Canfora, Corrado Aaron Visaggio, and Vito Paradiso</i>	

Availability and Reliability 2 (ARES Full Papers)

Improving Reliability for Multi-home Inbound Traffic: MHLB/I Packet-Level Inter-domain Load-Balancing	248
<i>Hiroshi Fujinoki</i>	

Proactive Resource Management for Failure Resilient High Performance Computing Clusters	257
<i>Song Fu and Cheng-Zhong Xu</i>	
A Perceptron Neural Network for Asymmetric Comparison-Based System-Level Fault Diagnosis	265
<i>Mourad Elhadef</i>	
Perfect Failure Detection in the Partitioned Synchronous Distributed System Model	273
<i>Raimundo José de Araújo Macêdo and Sérgio Gorender</i>	
Privacy and Trust (ARES Full Papers)	
Specification of Anonymity as a Secrecy Property in the ADM Logic - Homomorphic-Based Voting Protocols	281
<i>Mehdi Talbi, Valérie Viet Triem Tong, and Adel Bouhoula</i>	
Measuring Voter-Controlled Privacy	289
<i>Hugo Jonker, Sjouke Mauw, and Jun Pang</i>	
Generating User-Understandable Privacy Preferences	299
<i>Jan Kolter and Günther Pernul</i>	
An Automatic Privacy Policy Agreement Checker for E-services	307
<i>George O.M. Yee</i>	
Dependable Systems and Trusted Computing 1 (ARES Short Papers)	
A Micro-FT-UART for Safety-Critical SoC-Based Applications	316
<i>Mohammad-Hamed Razmkhah, Seyed Ghassem Miremadi, and Alireza Ejlali</i>	
MixVM - An Approach to Service Isolation and Data Protection in Mobile Context-Sensitive Applications	322
<i>Thomas Butter and Markus Aleksy</i>	
On the Security of Untrusted Memory	329
<i>Jörn-Marc Schmidt and Stefan Tillich</i>	
Dependable Systems and Trusted Computing 2 (ARES Short Papers)	
Detecting Image Tampering Using Feature Fusion	335
<i>Pin Zhang and Xiangwei Kong</i>	
SecMiLiA: An Approach in the Agent Protection	341
<i>Antonio Muñoz, Antonio Maña, and Daniel Serrano</i>	
Traffic Controller: A Practical Approach to Block Network Covert Timing Channel	349
<i>Yi Wang, Ping Chen, Yi Ge, Bing Mao, and Li Xie</i>	
Software Security (ARES Short Papers)	
Capturing Information Flow with Concatenated Dynamic Taint Analysis	355
<i>Hyung Chan Kim, Angelos D. Keromytis, Michael Covington, and Ravi Sahita</i>	
Risk-Driven Architectural Decomposition	363
<i>Thomas Heyman, Riccardo Scandariato, and Wouter Joosen</i>	
Reducing the Cost of Session Key Establishment	369
<i>Bezawada Bruhadeshwar, Kishore Kothapalli, and Maddi Sree Deepya</i>	

Privacy and Trust (ARES Short Papers)

Accuracy: The Fundamental Requirement for Voting Systems	374
<i>Tim Storer and Russell Lock</i>	
Reusable Security Requirements for Healthcare Applications	380
<i>Jostein Jensen, Inger Anne Tøndel, Martin Gilje Jaatun, Per Håkon Meland, and Herbjørn Andresen</i>	
P2F: A User-Centric Privacy Protection Framework	386
<i>Maryam Jafari-lafti, Chin-Tser Huang, and Csilla Farkas</i>	

Enterprise Security and Security Evaluation 1 (ARES Short Papers)

Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001	392
<i>Wolfgang Boehmer</i>	
Methodology for Experimental ICT Industrial and Critical Infrastructure Security Tests	400
<i>Marcelo Masera and Igor Nai Fovino</i>	
Ascertaining the Financial Loss from Non-dependable Events in Business Interactions by Using the Monte Carlo Method	406
<i>Omar Hussain and Tharam Dillon</i>	

Enterprise Security and Security Evaluation 2 (ARES Short Papers)

Building a Responsibility Model Including Accountability, Capability and Commitment	412
<i>Christophe Feltus and Michaël Petit</i>	
AVISPA in the Validation of Ambient Intelligence Scenarios	420
<i>Antonio Muñoz, Antonio Maña, and Daniel Serrano</i>	
Security Evaluation of an Intrusion Tolerant System with MRSPNs	427
<i>Ryutaro Fujimoto, Hiroyuki Okamura, and Tadashi Dohi</i>	
Algebraic Properties in Alice and Bob Notation	433
<i>Sebastian Mödersheim</i>	

Availability and Reliability (ARES Short Papers)

Scrubbing in Storage Virtualization Platform for Long-Term Backup Application	441
<i>Ao Ma, Yang Yin, Wenwu Na, Xiaoxuan Meng, Qingzhong Bu, and Lu Xu</i>	
Fault Tolerant and Low Energy Write-Back Heterogeneous Set Associative Cache for DSM Technologies	448
<i>Mehrtash Manoochehri, Alireza Ejlali, and Seyed Ghassem Miremadi</i>	
Generating AMF Configurations from Software Vendor Constraints and User Requirements	454
<i>A. Kanso, M. Toeroe, A. Hamou-Lhadj, and F. Khendek</i>	

Authentication and Authorization (ARES Short Papers)

Using XACML for Embedded and Fine-Grained Access Control Policy	462
<i>George Hsieh, Keith Foster, Gerald Emamali, Gregory Patrick, and Lisa Marvel</i>	
A-COLD: Access Control of Web OLAP over Multi-data Warehouse	469
<i>Somchart Fugkeaw, Piyawit Manpanpanich, and Sekpon Juntapremjitt</i>	
Package-Role Based Authorization Control Model for Wireless Network Services	475
<i>Huy Hoang Ngo, Xianping Wu, Phu Dung Le, and Campbell Wilson</i>	
Security Credential Mapping in Grids	481
<i>Mehran Ahsant, Esteban Talavera Gonzalez, and Jim Basney</i>	

Cryptography 1 (ARES Short Papers)

A Dynamic Attribute-Based Group Signature Scheme and its Application in an Anonymous Survey for the Collection of Attribute Statistics	487
<i>Keita Emura, Atsuko Miyaji, and Kazumasa Omote</i>	
Security in Quantum Networks as an Optimization Problem	493
<i>Stefan Rass and Peter Schartner</i>	
Finding Preimages of Multiple Passwords Secured with VSH	499
<i>Kimmo Halunen, Pauli Rikula, and Juha Rönning</i>	

Cryptography 2 (ARES Short Papers)

Choosing Parameters to Achieve a Higher Success Rate for Hellman Time Memory Trade Off Attack	504
<i>Nurdan Saran and Ali Doğanaksoy</i>	
Generalized Robust Combiners for Oblivious Transfer	510
<i>Ganugula Umadevi, Sarat C. Addepalli, and Kannan Srinathan</i>	

DAWAM 2009 - Security & Privacy Enhancement in DWHs

Including Security Rules Support in an MDA Approach for Secure DWs	516
<i>Carlos Blanco, Ignacio García-Rodríguez de Guzmán, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini</i>	
A System of Privacy Preserving Distributed Spatial Data Warehouse Using Relation Decomposition	522
<i>Marcin Gorawski and Szymon Panfil</i>	
Applying an MDA-Based Approach to Consider Security Rules in the Development of Secure DWs	528
<i>Carlos Blanco, Ignacio García-Rodríguez de Guzmán, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini</i>	

DAWAM 2009 - Intrusion and Network Attack Prevention

Identity-Based Hybrid Signcryption	534
<i>Fagen Li, Masaaki Shirase, and Tsuyoshi Takagi</i>	
Towards Intrusion Detection for Encrypted Networks	540
<i>Vik Tor Goh, Jacob Zimmermann, and Mark Looi</i>	

A Mobile Ambients-Based Approach for Network Attack Modelling and Simulation	546
<i>Virginia N.L. Franqueira, Pascal van Eck, Roel Wieringa, and Raul H.C. Lopes</i>	
DAWAM 2009 - Dependability, Failure Analysis & Detection	
Statistical Failure Analysis of a Web Server System	554
<i>Toshiya Fujii and Tadashi Dohi</i>	
A Policy Framework for Data Management in Services Marketplaces	560
<i>Jun Li, Bryan Stephenson, and Sharad Singhal</i>	
Modeling Misuse Patterns	566
<i>Eduardo B. Fernandez, Nobukazu Yoshioka, and Hironori Washizaki</i>	
Novel Algorithms for Subgroup Detection in Terrorist Networks	572
<i>Nasrullah Memon, Abdul Rasool Qureshi, Uffe Kock Wiil, and David L. Hicks</i>	
FARES 2009 - Authentication and Authorization	
QR-TAN: Secure Mobile Transaction Authentication	578
<i>Guenther Starnberger, Lorenz Froihofer, and Karl M. Goeschka</i>	
An Authentication Watermark Algorithm for JPEG images	584
<i>Xiaowei Shi, Fenlin Liu, Daofu Gong, and Jing Jing</i>	
A New Watermarking Attack Using Long-Range Correlation Image Restoration	589
<i>A.H. Taherinia, M. Fotouhi, and M. Jamzad</i>	
FARES 2009 - Security in Distributed Systems	
The Case for a Simpler Security Model in Grid Computing	595
<i>Frederik Orellana, Christian Ulrik Sottrup, Anders Wäänänen, Daniel Kalici, and Michael Grønager</i>	
Secured Multi-robotic Active Localization without Exchange of Maps: A Case of Secure Cooperation Amongst Non-trusting Robots	600
<i>Sarat C. Addepalli, Piyush Bansal, Kannan Srinathan, and K. Madhava Krishna</i>	
Position Paper: Secure Infrastructure for Scientific Data Life Cycle Management	606
<i>M. Descher, T. Feilhauer, T. Ludescher, P. Masser, B. Wenzel, P. Brezany, I. Elsayed, A. Woehrer, A.M. Tjoa, and D. Huemer</i>	
FARES 2009 - Software Security and Digital Forensics	
A Robust Image Watermarking Method in Wavelet Domain Using Genetic Algorithm	612
<i>S. Hamid Amiri and Mansour Jamzad</i>	
An Efficient Measurement of Object Oriented Design Vulnerability	618
<i>Alka Agrawal, Shalini Chandra, and Raees Ahmad Khan</i>	
FORVEST: A Support Tool for Formal Verification of Security Specifications with ISO/IEC 15408	624
<i>Kenichi Yajima, Shoichi Morimoto, Daisuke Horie, Noor Sheila Azreen, Yuichi Goto, and Jingde Cheng</i>	

FARES 2009 - Dependability Aspects

Using Hybrid Trust Model for Handling Inaccurate Resource	630
<i>Bagher Rahimpour Cami and Mohammad Reza Matash Brujerdi</i>	
A High Speed and Low Cost Error Correction Technique for the Carry Select Adder	635
<i>Alireza Namazi, Seyed Ghassem Miremadi, and Alireza Ejlali</i>	
An Improvement of REM: A Replication Oriented Event-Based Middleware	641
<i>Youcheng Chen, Mohammad Reza Selim, Yuichi Goto, and Jingde Cheng</i>	

GloSec 2009 - Session 1

Advanced Flooding Attack on a SIP Server	647
<i>Xianglin Deng and Malcolm Shore</i>	
State of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia	652
<i>Sopheak Cheang and Sinawong Sang</i>	
An Inclusive Information Society Needs a Global Approach of Information Security	658
<i>Solange Ghernaouti-Hélie</i>	

GloSec 2009 - Session 2

Measuring Peer-to-Peer Botnets Using Control Flow Stability	663
<i>Binbin Wang, Zhitang Li, Hao Tu, and Jie Ma</i>	
Regulatory Compliance and Information Security Assurance	670
<i>Igli Tashi</i>	
Information Security Optimization: From Theory to Practice	675
<i>David John Simms</i>	

IWSS 2009 - Security in Ad Hoc and Mesh Networks

Trusting User Defined Context in MANETs: Experience from the MIDAS Approach	681
<i>Vegar Westerlund, Thomas Pronstad, Inger Anne Tøndel, and Leendert Wienhofen</i>	
Deconvolving Protected Signals	687
<i>Mohaned Kafri and Sylvain Guilley</i>	

IWSS 2009 - Security in Contactless Systems

Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones	695
<i>Collin Mulliner</i>	
Post-Distribution Provisioning and Personalization of a Payment Application on a UICC-Based Secure Element	701
<i>Vincent Alimi and Marc Pasquet</i>	
A Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems	706
<i>George Pouloupoulos, Konstantinos Markantonakis, and Keith Mayes</i>	

OSA 2009 - Risk Management

A New Approach for the Construction of Fault Trees from System Simulink	712
<i>G. Latif-Shabgahi and F. Tajarrood</i>	
Estimating ToE Risk Level Using CVSS	718
<i>Siv Hilde Houmb and Virginia N.L. Franqueira</i>	
Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide	726
<i>Amril Syalim, Yoshiaki Hori, and Kouichi Sakurai</i>	

OSA 2009 - Security Management and Education

Haste in Knowledge-Intensive Work: A Major Threat to Information Security Management in Business Environments	732
<i>Juhani Anttila and Jorma Kajava</i>	
Standards-Based Cyber Exercises	738
<i>Ronald Dodge, Brian Hay, and Kara Nance</i>	
Patterns to Support the Development of Privacy Policies	744
<i>Luanna Lopes Lobato, Eduardo B. Fernandez, and Sergio Donizetti Zorzo</i>	

OSA 2009 - Security Mangement

Multidimensional Management of Information Security – A Metrics Based Approach Merging Business and Information Security Topics	750
<i>Sebastian Sowa and Roland Gabriel</i>	
A Security Management Assurance Model to Holistically Assess the Information Security Posture	756
<i>Igli Tashi and Solange Ghernaouti-Hélie</i>	
Methodology to Align Business and IT Policies: Use Case from an IT Company	762
<i>Christophe Feltus, Christophe Incoul, Jocelyn Aubert, Benjamin Gateau, André Adelsbach, and Marc Camy</i>	

RIBC 2009 - Authentication, Watermarking and Steganography

On the Higher Order Nonlinearities of Boolean Functions and S-boxes	768
<i>Claude Carlet</i>	
A Certificate Revocable Anonymous Authentication Scheme with Designated Verifier	769
<i>Keita Emura, Atsuko Miyaji, and Kazumasa Omote</i>	
A Standard MIDI File Steganography Based on Fluctuation of Duration	774
<i>Kotaro Yamamoto and Munetoshi Iwakiri</i>	
A Signature Scheme Associated with Universal Re-signcryption	780
<i>Kohei Tatara and Kouichi Sakurai</i>	

RIBC 2009 - Authentication, Watermarking and Cryptosystems

Real-Time Audio Watermarking with Wavetable Alternation in Digital Instrument	786
<i>Kotaro Yamamoto and Munetoshi Iwakiri</i>	
A Reconfigurable-Permutation Algorithm for M_S-Box	792
<i>Hiroshi Kudou, Shunn-ichiro Nakayama, Atsushi Watanabe, Tomoyuki Nagase, and Yoshio Yoshioka</i>	

SecSE 2009 - Education and Other Vulnerabilities

Protecting Global and Static Variables from Buffer Overflow Attacks	798
<i>Yves Younan, Frank Piessens, and Wouter Joosen</i>	
Static Code Analysis to Detect Software Security Vulnerabilities - Does Experience Matter?	804
<i>Dejan Baca, Kai Petersen, Bengt Carlsson, and Lars Lundberg</i>	
hACMEgame: A Tool for Teaching Software Security	811
<i>Øyvind Nerbråten and Lillian Røstad</i>	

SecSE 2009 - Secure Software-Development Lifecycles and Reuse

Towards Evaluation of Security Assurance during the Software Development Lifecycle	817
<i>Ilkka Uusitalo, Kaarina Karppinen, Pasi Ahonen, and Heimo Pentikäinen</i>	
An Architectural Foundation for Security Model Sharing and Reuse	823
<i>Per Håkon Meland, Shanai Ardi, Jostein Jensen, Erkuden Rios, Txus Sanchez, Nahid Shahmehri, and Inger Anne Tøndel</i>	
A Knowledge Management Approach to Support a Secure Software Development	829
<i>Francisco José Barreto Nunes, Arnaldo Dias Belchior, and Adriano Bessa Albuquerque</i>	

SecSE 2009 - Model-Driven Development and Checklists

A Practical Framework for the Dataflow Pointcut in AspectJ	835
<i>Amine Boukhtouta, Dima Alhadidi, and Mourad Debbabi</i>	
SecureMDD: A Model-Driven Development Method for Secure Smart Card Applications	841
<i>Nina Moebius, Kurt Stenzel, Holger Grandy, and Wolfgang Reif</i>	
Linking Privacy Solutions to Developer Goals	847
<i>Kim Wuyts, Riccardo Scandariato, Bart De Decker, and Wouter Joosen</i>	
Software Inspections Using Guided Checklists to Ensure Security Goals	853
<i>Frank Elberzhager, Alexander Klaus, and Marek Jawurek</i>	

SecUSAB 2009 - Session 1

Managing Rights and Value of Digital Media	859
<i>Filippo Chiariglione, Giacomo Cosenza, and Sergio Matone</i>	
A Criteria-Based Evaluation Framework for Authentication Schemes in IMS	865
<i>Charlott Eliasson, Markus Fiedler, and Ivar Jørstad</i>	

The User-Centric Vision Matches Credentials Exchanges	870
<i>Mikaël Ates, Jacques Fayolle, Christophe Gravier, and Jeremy Lardon</i>	
SecUSAB 2009 - Session 2	
Patient-Administered Access Control: A Usability Study	877
<i>Lillian Røstad and Ole Andreas Alsos</i>	
An Experimental System for Studying the Tradeoff between Usability and Security	882
<i>Noam Ben-Asher, Joachim Meyer, Sebastian Möller, and Roman Englert</i>	
WAIS 2009 - Security Analysis	
Rank Swapping for Partial Orders and Continuous Variables	888
<i>Vicenç Torra</i>	
An Improved Authentication Protocol Based on One-Way Hash Functions and Diffie-Hellman Key Exchange	894
<i>Marko Hölbl and Tatjana Welzer</i>	
Security Analysis for P2P Routing Protocols	899
<i>Tatsuro Fujii, Yizhi Ren, Yoshiaki Hori, and Kouichi Sakurai</i>	
WAIS 2009 - Network Security	
Secrecy Capacity of Wireless LAN	905
<i>Ryuzou Nishi, Yoshiaki Hori, and Kouichi Sakurai</i>	
Privacy-Preserving Collaborative Filtering Schemes	911
<i>Hiroaki Kikuchi, Hiroyasu Kizawa, and Minako Tada</i>	
A Framework for Understanding Botnets	917
<i>Justin Leonard, Shouhuai Xu, and Ravi Sandhu</i>	
WAIS 2009 - Signature and Protection	
Enterprise-Oriented Digital Rights Management Mechanism: eDRM	923
<i>Chia-Chen Lin, Shih-Chi Wu, Po-Hsuan Chiang, and Chang-Chi Chen</i>	
Utility and Risk of JPEG-Based Continuous Microdata Protection Methods	929
<i>Javier Jiménez and Vicenç Torra</i>	
Towards Efficient ID-Based Signature Schemes with Batch Verifications from Bilinear Pairings	935
<i>Yuh-Min Tseng, Tsu-Yang Wu, and Jui-Di Wu</i>	
Yet Another Sanitizable Signature from Bilinear Maps	941
<i>Tetsuya Izu, Noboru Kunihiro, Kazuo Ohta, Makoto Sano, and Masahiko Takenaka</i>	
WAIS 2009 - Secure Systems	
Generation of Prototypes for Masking Sequences of Events	947
<i>Aida Valls, Cristina Gómez-Alonso, and Vicenç Torra</i>	
Enhancing Control of Service Compositions in Service-Oriented Architectures	953
<i>Christian Schneider, Frederic Stumpf, and Claudia Eckert</i>	
Truly Anonymous Paper Submission and Review Scheme	960
<i>Chun-I Fan, Ming-Te Chen, and Lung-Hsien Chen</i>	

An Implementation of the Binding Mechanism in the Web Browser for Preventing XSS Attacks: Introducing the Bind-Value Headers	966
<i>Genta Iha and Hiroshi Doi</i>	

WAIS 2009 - Information Security

Polymorphic Worm Detection by Analyzing Maximum Length of Instruction Sequence in Network Packets	972
<i>Kohei Tatara, Yoshiaki Hori, and Kouichi Sakurai</i>	
Automated Instruction-Set Randomization for Web Applications in Diversified Redundant Systems	978
<i>Frédéric Majorczyk and Jonathan-Christofer Demay</i>	
An Improvement to a Decentralized Management Method for Uniquely Accessible Attribute Information	984
<i>Yoshio Kakizaki, Yoshiaki Yoshida, and Hidekazu Tsuji</i>	
Making Use of Human Visual Capability to Improve Information Security	990
<i>Masakatsu Nishigaki and Takumi Yamamoto</i>	

WSDF 2009 - Digital Forensics 1

Enhancement of Forensic Computing Investigations through Memory Forensic Techniques	995
<i>Matthew Simon and Jill Slay</i>	
Improving Performance in Digital Forensics: A Case Using Pattern Matching Board	1001
<i>Jooyoung Lee, Sungkyung Un, and Dowon Hong</i>	
Computer Forensics in Japan: A Preliminary Study	1006
<i>Jigang Liu and Tetsutaro Uehara</i>	

WSDF 2009 - Digital Forensics 2

Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation	1012
<i>Grant Osborne and Benjamin Turnbull</i>	
A Post-Mortem Incident Modeling Method	1018
<i>Shanai Ardi and Nahid Shahmehri</i>	
Investigating the Implications of Virtual Machine Introspection for Digital Forensics	1024
<i>Kara Nance, Matt Bishop, and Brian Hay</i>	

Author Index