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
Distributed Systems and Grid (ARES Full Papers)

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

SOA Security (ARES Full Papers)

The Accountability Problem of Flooding Attacks in Service-Oriented Architectures ...............................25
   Meiko Jensen and Jörg Schwenk
Web Service Trust: Towards a Dynamic Assessment Framework ..........................................................33
   George Spanoudakis and Stephane LoPresti
   Michael Menzel, Ivonne Thomas, and Christoph Meinel
Enterprise Security 1 (ARES Full Papers)

Quantitative Analysis of Secure Information Flow via Probabilistic Semantics .................................................................49
  Chunyan Mu and David Clark

Deploying Security Policy in Intra and Inter Workflow Management Systems ...............................................................58
  Samiha Ayed, Nora Cuppens-Boulahia, and Frédéric Cuppens

An Empirically Derived Loss Taxonomy Based on Publicly Known Security Incidents ..................................................66
  Frank Innerhofer-Oberperfler and Ruth Breu

Intrusion and Fraud Detection (ARES Full Papers)

Defeating Dynamic Data Kernel Rootkit Attacks via VMM-Based Guest-Transparent Monitoring ......................................................74
  Junghwan Rhee, Ryan Riley, Dongyan Xu, and Xuxian Jiang

Server-Side Prediction of Source IP Addresses Using Density Estimation ................................................................................82
  Markus Goldstein, Matthias Reif, Armin Stahl, and Thomas Breuel

Detecting Stepping-Stone Connection Using Association Rule Mining ..................................................................................90
  Ying-wei Kuo and Shou-Hsuan Stephen Huang

Enterprise Security 2 (ARES Full Papers)

Formal Analyses of Usage Control Policies ..........................................................................................................................98
  Alexander Pretschner, Judith Rüesch, Christian Schaefer, and Thomas Walter

A First Step towards Characterizing Stealthy Botnets .................................................................106
  Justin Leonard, Shouhuai Xu, and Ravi Sandhu

Intrusion Process Modeling for Security Quantification .........................................................................................................114
  Jaafar Almasizadeh and Mohammad Abdollahi Azgomi

Different Approaches to In-House Identity Management - Justification of an Assumption ................................................122
  L. Fuchs, C. Broser, and G. Pernul

Digital Forensics and Security in Communication (ARES Full Papers)

An LPN-Problem-Based Lightweight Authentication Protocol for Wireless Communications ......................................................130
  Ya-Fen Chang and Yen-Cheng Lai

Revealing the Calling History of SIP VoIP Systems by Timing Attacks ..............................................................................135
  Ge Zhang, Simone Fischer-Huebner, Leonardo A. Martucci, and Sven Ehlert

The Anatomy of Electronic Evidence – Quantitative Analysis of Police E-Crime Data .....................................................143
  Benjamin Turnbull, Robert Taylor, and Barry Blundell

A Robust Image Watermarking Using Two Level DCT and Wavelet Packets Denoising ......................................................150
  A.H. Taherinia and M. Jamzad
Availability and Reliability 1 (ARES Full Papers)
On Equilibrium Distribution Properties in Software Reliability Modeling .................................................................158
    Xiao Xiao and Tadashi Dohi
An Analysis of Fault Effects and Propagations in AVR Microcontroller
ATmega103(L) ...........................................................................................................................................................166
    Alireza Rohani and Hamid. R. Zarandi
Blue Gene/L Log Analysis and Time to Interrupt Estimation ....................................................................................173
    Narate Taerat, Nichamon Naksinehaboon, Clayton Chandler, James Elliott,
    Chokchai Leangsukson, George Ostrouchov, Stephen L. Scott, and Christian Engelmann

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

Software Security 1 (ARES Full Papers)
Prioritisation and Selection of Software Security Activities ......................................................................................201
    David Byers and Nahid Shahmehri
BRICK: A Binary Tool for Run-Time Detecting and Locating Integer-Based Vulnerability ........................................208
    Ping Chen, Yi Wang, Zhi Xin, Bing Mao, and Li Xie
Enhancing Automated Detection of Vulnerabilities in Java Components .............................................................216
    Pierre Parrend

Software Security 2 (ARES Full Papers)
Automated Support for Security Requirements Engineering in Software Product Line
Domain Engineering .........................................................................................................................................................224
    Daniel Mellado, Jesus Rodriguez, Eduardo Fernández-Medina, and Mario Piattini
Identifying and Resolving Least Privilege Violations in Software Architectures ..................................................232
    Koen Buyens, Bart De Win, and Wouter Joosen
A Test Framework for Assessing Effectiveness of the Data Privacy Policy’s Implementation into Relational Databases .................................................................................................................................240
    Gerardo Canfora, Corrado Aaron Visaggio, and Vito Paradiso

Availability and Reliability 2 (ARES Full Papers)
Improving Reliability for Multi-home Inbound Traffic: MHLB/I Packet-Level
Inter-domain Load-Balancing .....................................................................................................................................248
    Hiroshi Fujinoki
Proactive Resource Management for Failure Resilient High Performance Computing Clusters ................................................................. 257
   Song Fu and Cheng-Zhong Xu
A Perceptron Neural Network for Asymmetric Comparison-Based System-Level Fault Diagnosis ....................................................................................... 265
   Mourad Elhadef
Perfect Failure Detection in the Partitioned Synchronous Distributed System Model ................................................. 273
   Raimundo José de Araújo Macêdo and Sérgio Gorender

Privacy and Trust (ARES Full Papers)
Specification of Anonymity as a Secrecy Property in the ADM Logic -
Homomorphic-Based Voting Protocols ................................................................. 281
   Mehdi Talbi, Valérie Viet Triem Tong, and Adel Bouhoula
Measuring Voter-Controlled Privacy .............................................................................. 289
   Hugo Jonker, Sjouke Mauw, and Jun Pang
Generating User-Understandable Privacy Preferences ......................................................................................... 299
   Jan Kolter and Günther Pernul
An Automatic Privacy Policy Agreement Checker for E-services .................................................. 307
   George O.M. Yee

Dependable Systems and Trusted Computing 1 (ARES Short Papers)
A Micro-FT-UART for Safety-Critical Soc-Based Applications .................................................. 316
   Mohammad-Hamed Razmkhah, Seyed Ghassem Miremadi, and Alireza Ejlali
MixVM - An Approach to Service Isolation and Data Protection in Mobile Context-Sensitive Applications .................................................. 322
   Thomas Butter and Markus Aleksy
On the Security of Untrusted Memory .................................................................................. 329
   Jörn-Marc Schmidt and Stefan Tillich

Dependable Systems and Trusted Computing 2 (ARES Short Papers)
Detecting Image Tampering Using Feature Fusion ................................................................ 335
   Pin Zhang and Xiangwei Kong
SecMiLiA: An Approach in the Agent Protection ................................................................................ 341
   Antonio Muñoz, Antonio Mañia, and Daniel Serrano
Traffic Controller: A Practical Approach to Block Network Covert Timing Channel ............................................. 349
   Yi Wang, Ping Chen, Yi Ge, Bing Mao, and Li Xie

Software Security (ARES Short Papers)
Capturing Information Flow with Concatenated Dynamic Taint Analysis .................................................. 355
   Hyung Chan Kim, Angelos D. Keromytis, Michael Covington, and Ravi Sahita
Risk-Driven Architectural Decomposition ................................................................................ 363
   Thomas Heyman, Riccardo Scandariato, and Wouter Joosen
Reducing the Cost of Session Key Establishment .................................................................................. 369
   Bezawada Bruhadeshwar, Kishore Kothapalli, and Maddi Sree Deepya
Privacy and Trust (ARES Short Papers)

Accuracy: The Fundamental Requirement for Voting Systems ................................................................. 374
    Tim Storer and Russell Lock

Reusable Security Requirements for Healthcare Applications ........................................................................ 380
    Jostein Jensen, Inger Anne Tøndel, Martin Gilje Jaatun, Per Håkon Meland, and Herbjørn Andresen

P2F: A User-Centric Privacy Protection Framework .................................................................................... 386
    Maryam Jafari-lafti, Chin-Tser Huang, and Csilla Farkas

Enterprise Security and Security Evaluation 1 (ARES Short Papers)

Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001 .............................................................. 392
    Wolfgang Boehmer

Methodology for Experimental ICT Industrial and Critical Infrastructure Security Tests .......................................................... 400
    Marcelo Masera and Igor Nai Fovino

Ascertaining the Financial Loss from Non-dependable Events in Business Interactions by Using the Monte Carlo Method ........................................................................................................... 406
    Omar Hussain and Tharam Dillon

Enterprise Security and Security Evaluation 2 (ARES Short Papers)

Building a Responsibility Model Including Accountability, Capability and Commitment ........................................... 412
    Christophe Feltus and Michaël Petit

AVISPA in the Validation of Ambient Intelligence Scenarios ........................................................................ 420
    Antonio Muñoz, Antonio Maña, and Daniel Serrano

Security Evaluation of an Intrusion Tolerant System with MRSPNs .............................................................. 427
    Ryutaro Fujimoto, Hiroyuki Okamura, and Tadashi Dohi

Algebraic Properties in Alice and Bob Notation ............................................................................................... 433
    Sebastian Mödersheim

Availability and Reliability (ARES Short Papers)

Scrubbing in Storage Virtualization Platform for Long-Term Backup Application ........................................ 441
    Ao Ma, Yang Yin, Wenwu Na, Xiaoxuan Meng, Qingzhong Bu, and Lu Xu

Fault Tolerant and Low Energy Write-Back Heterogeneous Set Associative Cache for DSM Technologies .......................................................... 448
    Mehrtash Manoochehri, Alireza Ejlali, and Seyed Ghassem Miremadi

Generating AMF Configurations from Software Vendor Constraints and User Requirements ................................ 454
**Authentication and Authorization (ARES Short Papers)**

Using XACML for Embedded and Fine-Grained Access Control Policy ................................................................. 462
  *George Hsieh, Keith Foster, Gerald Emamali, Gregory Patrick, and Lisa Marvel*

A-COLD: Access Control of Web OLAP over Multi-data Warehouse .......................................................... 469
  *Somchart Fugkeaw, Piyawit Manpanpanich, and Sekpon Juntapremjitt*

Package-Role Based Authorization Control Model for Wireless Network Services ......................................... 475
  *Huy Hoang Ngo, Xianping Wu, Phu Dung Le, and Campbell Wilson*

Security Credential Mapping in Grids .................................................................................................................. 481
  *Mehran Ahsant, Esteban Talavera Gonzalez, and Jim Basney*

**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
  *Keita Emura, Atsuko Miyaji, and Kazumasa Omote*

Security in Quantum Networks as an Optimization Problem ........................................................................... 493
  *Stefan Rass and Peter Schartner*

Finding Preimages of Multiple Passwords Secured with VSH ........................................................................ 499
  *Kimmo Halunen, Pauli Rikula, and Juha Röning*

**Cryptography 2 (ARES Short Papers)**

Choosing Parameters to Achieve a Higher Success Rate for Hellman Time Memory Trade Off Attack .............................................................................................................................. 504
  *Nurdan Saran and Ali Doğanaksoy*

Generalized Robust Combiners for Oblivious Transfer .................................................................................... 510
  *Ganugula Umadevi, Sarat C. Addepalli, and Kannan Srinathan*

**DAWAM 2009 - Security & Privacy Enhancement in DWHs**

Including Security Rules Support in an MDA Approach for Secure DWs ........................................................... 516
  *Carlos Blanco, Ignacio García-Rodríguez de Guzmán, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini*

A System of Privacy Preserving Distributed Spatial Data Warehouse Using Relation Decomposition .................................................................................................................................................. 522
  *Marcin Gorawski and Szymon Panfil*

Applying an MDA-Based Approach to Consider Security Rules in the Development of Secure DWs .................................................................................................................................................. 528
  *Carlos Blanco, Ignacio García-Rodríguez de Guzmán, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini*

**DAWAM 2009 - Intrusion and Network Attack Prevention**

Identity-Based Hybrid Signcryption .................................................................................................................. 534
  *Fagen Li, Masaaki Shirase, and Tsuyoshi Takagi*

Towards Intrusion Detection for Encrypted Networks ....................................................................................... 540
  *Vik Tor Goh, Jacob Zimmermann, and Mark Looi*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Mobile Ambients-Based Approach for Network Attack Modelling and Simulation</td>
<td>546</td>
</tr>
<tr>
<td>Virginia N.L. Franqueira, Pascal van Eck, Roel Wieringa, and Raul H.C. Lopes</td>
<td></td>
</tr>
<tr>
<td>DAWAM 2009 - Dependability, Failure Analysis &amp; Detection</td>
<td>552</td>
</tr>
<tr>
<td>Statistical Failure Analysis of a Web Server System</td>
<td>554</td>
</tr>
<tr>
<td>Toshiya Fujii and Tadashi Dohi</td>
<td></td>
</tr>
<tr>
<td>A Policy Framework for Data Management in Services Marketplaces</td>
<td>560</td>
</tr>
<tr>
<td>Jun Li, Bryan Stephenson, and Sharad Singhal</td>
<td></td>
</tr>
<tr>
<td>Modeling Misuse Patterns</td>
<td>566</td>
</tr>
<tr>
<td>Eduardo B. Fernandez, Nobukazu Yoshioka, and Hironori Washizaki</td>
<td></td>
</tr>
<tr>
<td>Novel Algorithms for Subgroup Detection in Terrorist Networks</td>
<td>572</td>
</tr>
<tr>
<td>Nasrullah Memon, Abdul Rasool Qureshi, Uffe Kock Wiil, and David L. Hicks</td>
<td></td>
</tr>
<tr>
<td>FARES 2009 - Authentication and Authorization</td>
<td>578</td>
</tr>
<tr>
<td>QR-TAN: Secure Mobile Transaction Authentication</td>
<td></td>
</tr>
<tr>
<td>Guenther Starnberger, Lorenz Froihofer, and Karl M. Goeschka</td>
<td></td>
</tr>
<tr>
<td>An Authentication Watermark Algorithm for JPEG images</td>
<td>584</td>
</tr>
<tr>
<td>Xiaowei Shi, Fenlin Liu, Daofu Gong, and Jing Jing</td>
<td></td>
</tr>
<tr>
<td>A New Watermarking Attack Using Long-Range Correlation Image Restoration</td>
<td>589</td>
</tr>
<tr>
<td>A.H. Taherinia, M. Fotouhi, and M. Jamzad</td>
<td></td>
</tr>
<tr>
<td>FARES 2009 - Security in Distributed Systems</td>
<td>595</td>
</tr>
<tr>
<td>The Case for a Simpler Security Model in Grid Computing</td>
<td></td>
</tr>
<tr>
<td>Frederik Orellana, Christian Ulrik Sottrup, Anders Wäänänen, Daniel Kalici, and Michael Grønager</td>
<td></td>
</tr>
<tr>
<td>Secured Multi-robotic Active Localization without Exchange of Maps: A Case of Secure Cooperation Amongst Non-trusting Robots</td>
<td>600</td>
</tr>
<tr>
<td>Sarat C. Addepalli, Piyush Bansal, Kannan Srinathan, and K. Madhava Krishna</td>
<td></td>
</tr>
<tr>
<td>Position Paper: Secure Infrastructure for Scientific Data Life Cycle Management</td>
<td>606</td>
</tr>
<tr>
<td>FARES 2009 - Software Security and Digital Forensics</td>
<td>612</td>
</tr>
<tr>
<td>A Robust Image Watermarking Method in Wavelet Domain Using Genetic Algorithm</td>
<td></td>
</tr>
<tr>
<td>S. Hamid Amiri and Mansour Jamzad</td>
<td></td>
</tr>
<tr>
<td>An Efficient Measurement of Object Oriented Design Vulnerability</td>
<td>618</td>
</tr>
<tr>
<td>Alka Agrawal, Shalini Chandra, and Raees Ahmad Khan</td>
<td></td>
</tr>
<tr>
<td>FORVEST: A Support Tool for Formal Verification of Security Specifications with ISO/IEC 15408</td>
<td>624</td>
</tr>
<tr>
<td>Kenichi Yajima, Shoichi Morimoto, Daisuke Horie, Noor Sheila Azreen, Yuichi Goto, and Jingde Cheng</td>
<td></td>
</tr>
</tbody>
</table>
FARES 2009 - Dependability Aspects
Using Hybrid Trust Model for Handling Inaccurate Resource .........................................................630
   Bagher Rahimpour Cami and Mohammad Reza Matash Brujerdi
A High Speed and Low Cost Error Correction Technique for the Carry Select Adder ..................635
   Alireza Namazi, Seyed Ghassem Miremadi, and Alireza Ejlali
An Improvement of REM: A Replication Oriented Event-Based Middleware ................................641
   Youcheng Chen, Mohammad Reza Selim, Yuichi Goto, and Jingde Cheng

GloSec 2009 - Session 1
Advanced Flooding Attack on a SIP Server ......................................................................................647
   Xianglin Deng and Malcolm Shore
State of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia ..................652
   Sopheak Cheang and Sinawong Sang
   Solange Ghernaouti-Hélie

GloSec 2009 - Session 2
Measuring Peer-to-Peer Botnets Using Control Flow Stability ......................................................663
   Binbin Wang, Zhitang Li, Hao Tu, and Jie Ma
Regulatory Compliance and Information Security Assurance .........................................................670
   Igli Tashi
Information Security Optimization: From Theory to Practice .........................................................675
   David John Simms

IWSS 2009 - Security in Ad Hoc and Mesh Networks
Trusting User Defined Context in MANETs: Experience from the MIDAS Approach ..................681
   Vegar Westerlund, Thomas Pronstad, Inger Anne Tøndel, and Leendert Wienhofen
Deconvolving Protected Signals .......................................................................................................687
   Mohaned Kafi and Sylvain Guilley

IWSS 2009 - Security in Contactless Systems
Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones ..............................................695
   Collin Mulliner
Post-Distribution Provisioning and Personalization of a Payment Application on a UICC-Based Secure Element .................................................................701
   Vincent Alimi and Marc Pasquet
A Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems ..................706
   George Poulopoulos, Konstantinos Markantonakis, and Keith Mayes
OSA 2009 - Risk Management

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

OSA 2009 - Security Management and Education

  Juhani Anttila and Jorma Kajava
Standards-Based Cyber Exercises .............................................................. 738
  Ronald Dodge, Brian Hay, and Kara Nance
Patterns to Support the Development of Privacy Policies ........................................... 744
  Luanna Lopes Lobato, Eduardo B. Fernandez, and Sergio Donizetti Zorzo

OSA 2009 - Security Management

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

RIBC 2009 - Authentication, Watermarking and Steganography

On the Higher Order Nonlinearities of Boolean Functions and S-boxes .......................................................... 768
  Claude Carlet
A Certificate Revocable Anonymous Authentication Scheme with Designated Verifier ...................................................... 769
  Keita Emura, Atsuko Miyaji, and Kazumasa Omote
A Standard MIDI File Steganography Based on Fluctuation of Duration .......................................................... 774
  Kotaro Yamamoto and Munetoshi Iwakiri
A Signature Scheme Associated with Universal Re-signcryption ........................................... 780
  Kohei Tatara and Kouichi Sakurai
RIBC 2009 - Authentication, Watermarking and Cryptosystems

Real-Time Audio Watermarking with Wavetable Alternation in Digital Instrument ................................................................. 786
  Kotaro Yamamoto and Munetoshi Iwakiri

A Reconfigurable-Permutation Algorithm for M-S-Box ............................................................................................................. 792
  Hiroshi Kudou, Shunn-ichiro Nakayama, Atsushi Watanabe, Tomoyuki Nagase,
  and Yoshio Yoshioka

SecSE 2009 - Education and Other Vulnerabilities

Protecting Global and Static Variables from Buffer Overflow Attacks .......................................................................................... 798
  Yves Younan, Frank Piessens, and Wouter Joosen

  Dejan Baca, Kai Petersen, Bengt Carlsson, and Lars Lundberg

hACMEgame: A Tool for Teaching Software Security ............................................................................................................. 811
  Øyvind Nerbråten and Lillian Røstad

SecSE 2009 - Secure Software-Development Lifecycles and Reuse

Towards Evaluation of Security Assurance during the Software Development Lifecycle ........................................................................ 817
  Ilkka Uusitalo, Kaarina Karppinen, Pasi Ahonen, and Heimo Pentikäinen

An Architectural Foundation for Security Model Sharing and Reuse ............................................................................................... 823
  Per Håkon Meland, Shanai Ardi, Jostein Jensen, Erkuden Rios, Txus Sanchez,
  Nahid Shahmehri, and Inger Anne Tøndel

A Knowledge Management Approach to Support a Secure Software Development ............................................................................. 829
  Francisco José Barreto Nunes, Arnaldo Dias Belchior, and Adriano Bessa Albuquerque

SecSE 2009 - Model-Driven Development and Checklists

A Practical Framework for the Dataflow Pointcut in AspectJ .................................................................................................. 835
  Amine Boukhtouta, Dima Alhadidi, and Mourad Debbabi

SecureMDD: A Model-Driven Development Method for Secure Smart Card Applications ....................................................................... 841
  Nina Moebius, Kurt Stenzel, Holger Grandy, and Wolfgang Reif

Linking Privacy Solutions to Developer Goals ............................................................................................................................... 847
  Kim Wuyts, Riccardo Scandariato, Bart De Decker, and Wouter Joosen

Software Inspections Using Guided Checklists to Ensure Security Goals .......................................................................................... 853
  Frank Elberzhager, Alexander Klaus, and Marek Javurek

SecUSAB 2009 - Session 1

Managing Rights and Value of Digital Media ................................................................................................................................. 859
  Filippo Chiariglione, Giacomo Cosenza, and Sergio Matone

A Criteria-Based Evaluation Framework for Authentication Schemes in IMS ............................................................................. 865
  Charlott Eliasson, Markus Fiedler, and Ivar Jørstad
The User-Centric Vision Matches Credentials Exchanges .................................................................870
  Mikaël Ates, Jacques Fayolle, Christophe Gravier, and Jeremy Lardon

SecUSAB 2009 - Session 2

Patient-Administered Access Control: A Usability Study .................................................................877
  Lillian Røstad and Ole Andreas Alsos
An Experimental System for Studying the Tradeoff between Usability and Security .......................882
  Noam Ben-Asher, Joachim Meyer, Sebastian Möller, and Roman Englert

WAIS 2009 - Security Analysis

Rank Swapping for Partial Orders and Continuous Variables ...........................................................888
  Vicenç Torra
An Improved Authentication Protocol Based on One-Way Hash Functions and Diffie-Hellman Key Exchange ...........................................................................................................894
  Marko Hölbl and Tatjana Welzer
Security Analysis for P2P Routing Protocols .....................................................................................899
  Tatsuro Fujii, Yizhi Ren, Yoshiaki Hori, and Kouichi Sakurai

WAIS 2009 - Network Security

Secrecy Capacity of Wireless LAN .........................................................................................................905
  Ryuzou Nishi, Yoshiaki Hori, and Kouichi Sakurai
Privacy-Preserving Collaborative Filtering Schemes ...........................................................................911
  Hiroaki Kikuchi, Hiroyasu Kizawa, and Minako Tada
A Framework for Understanding Botnets ...........................................................................................917
  Justin Leonard, Shouhuai Xu, and Ravi Sandhu

WAIS 2009 - Signature and Protection

Enterprise-Oriented Digital Rights Management Mechanism: eDRM ................................................923
  Chia-Chen Lin, Shih-Chi Wu, Po-Hsuan Chiang, and Chang-Chi Chen
Utility and Risk of JPEG-Based Continuous Microdata Protection Methods ......................................929
  Javier Jiménez and Vicenç Torra
Towards Efficient ID-Based Signature Schemes with Batch Verifications .........................................935
  Yuh-Min Tseng, Tsu-Yang Wu, and Jui-Di Wu
Yet Another Sanitizable Signature from Bilinear Maps .........................................................................941
  Tetsuya Izu, Noboru Kunihiro, Kazuo Ohta, Makoto Sano, and Masahiko Takenaka

WAIS 2009 - Secure Systems

Generation of Prototypes for Masking Sequences of Events ................................................................947
  Aida Valls, Cristina Gómez-Alonso, and Vicenç Torra
Enhancing Control of Service Compositions in Service-Oriented Architectures ..................................953
  Christian Schneider, Frederic Stumpf, and Claudia Eckert
Truly Anonymous Paper Submission and Review Scheme ....................................................................960
  Chun-I Fan, Ming-Te Chen, and Lung-Hsien Chen
An Implementation of the Binding Mechanism in the Web Browser for Preventing XSS Attacks: Introducing the Bind-Value Headers .................................................................966

Genta Iha and Hiroshi Doi

WAIS 2009 - Information Security

Polymorphic Worm Detection by Analyzing Maximum Length of Instruction Sequence in Network Packets ...........................................................................................................972

Kohei Tatara, Yoshiaki Hori, and Kouichi Sakurai

Automated Instruction-Set Randomization for Web Applications in Diversified Redundant Systems ............................................................................................................................978

Frédéric Majorczyk and Jonathan-Christofer Demay

An Improvement to a Decentralized Management Method for Uniquely Accessible Attribute Information .................................................................................................................984

Yoshio Kakizaki, Yoshiaki Yoshida, and Hidekazu Tsuji

Making Use of Human Visual Capability to Improve Information Security .................................................................................................................................990

Masakatsu Nishigaki and Takumi Yamamoto

WSDF 2009 - Digital Forensics 1

Enhancement of Forensic Computing Investigations through Memory Forensic Techniques ..........................................................................................................................995

Matthew Simon and Jill Slay

Improving Performance in Digital Forensics: A Case Using Pattern Matching Board ............................................................................................................1001

Jooyoung Lee, Sungkyung Un, and Dowon Hong

Computer Forensics in Japan: A Preliminary Study ..........................................................................................................................1006

Jigang Liu and Tetsutaro Uehara

WSDF 2009 - Digital Forensics 2

Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation ..........................................................................................................................1012

Grant Osborne and Benjamin Turnbull

A Post-Mortem Incident Modeling Method ..........................................................................................................................1018

Shanai Ardi and Nahid Shahmehri

Investigating the Implications of Virtual Machine Introspection for Digital Forensics ..........................................................................................................................1024

Kara Nance, Matt Bishop, and Brian Hay

Author Index