

# **2010 International Conference on Availability, Reliability and Security**

**(ARES 2010)**

**Krakow, Poland  
15-18 February 2010**



IEEE Catalog Number: CFP1039A-PRT  
ISBN: 978-1-4244-5879-0

# 2010 International Conference on Availability, Reliability and Security

---

## *ARES 2010*

# Table of Contents

Welcome Message from ARES 2010 Chairs.....	xv
Welcome Message from ARES 2010 Workshop Co-Chair.....	xvi
ARES 2010 Conference Officers.....	xvii
ARES 2010 Reviewer List.....	xviii
Welcome Message from the FARES 2010 Workshop C0-Chairs.....	xxi
Welcome Message from the OSA 2010 Workshop Chair.....	xxii
OSA 2010 Organizing Committee.....	xxiii
OSA 2010 Reviewer List.....	xxiv
Welcome Message from the SECSE 2010 Workshop Organizers.....	xxv
SecSE 2010 Organization.....	xxvi
Welcome Message from the SPattern 2010 Workshop Organizers.....	xxvii
SPattern 2010 Organization Committee.....	xxviii
Welcome Message from the WAIS 2010 Workshop Chair.....	xxix
WAIS 2010 Organizing Committee.....	xxx
WAIS 2010 Reviewers.....	xxxi
Welcome Message from the WSDF 2010 Workshop Organizers.....	xxxii
WSDF 2010 Organizing Committee.....	xxxiii

---

## **ARES 2010 Full Papers**

### **Network Security I**

A Security Decision-Reaction Architecture for Heterogeneous Distributed Network .....	1
<i>Christophe Feltus, Djamel Khadraoui, and Jocelyn Aubert</i>	
Dual-Level Attack Detection and Characterization for Networks under DDoS .....	9
<i>Anjali Sardana and Ramesh Chandra Joshi</i>	
Improving Effectiveness of Intrusion Detection by Correlation Feature Selection .....	17
<i>Hai Nguyen, Katrin Franke, and Slobodan Petrovic</i>	

### **Network Security II**

Analytical Approach to Attack Graph Analysis for Network Security .....	25
<i>Phongphun Kijsanayothin and Rattikorn Hewett</i>	
Affects of Queuing Mechanisms on RTP Traffic: Comparative Analysis of Jitter, End-to-End Delay and Packet Loss .....	33
<i>Gregory Epiphaniou, Carsten Maple, Paul Sant, and Matthew Reeve</i>	
A Computer Architecture with Hardwarebased Malware Detection .....	41
<i>Klaus Hildebrandt, Igor Podebrad, and Bernd Klauer</i>	

### **Identity Management, Authentication, and Authorization I**

Solving the Transitive Access Problem for the Services Oriented Architecture .....	46
<i>Alan H. Karp and Jun Li</i>	
Unified Public Key Infrastructure Supporting Both Certificate-Based and ID-Based Cryptography .....	54
<i>Byoungcheon Lee</i>	
Secure Bindings of SAML Assertions to TLS Sessions .....	62
<i>Florian Kohlar, Jörg Schwenk, Meiko Jensen, and Sebastian Gajek</i>	

### **Identity Management, Authentication, and Authorization II**

From Contextual Permission to Dynamic Pre-obligation: An Integrated Approach .....	70
<i>Yehia Elrakaiby, Frédéric Cuppens, and Nora Cuppens-Boulahia</i>	
2-clickAuth—Optical Challenge-Response Authentication .....	79
<i>Anna Vapen, David Byers, and Nahid Shahmehri</i>	
Architecture-Aware Adaptive Deployment of Contextual Security Policies .....	87
<i>Stere Preda, Nora Cuppens-Boulahia, Frédéric Cuppens, and Laurent Toutain</i>	

## Availability and Reliability I

Using Smart Cards for Tamper-Proof Timestamps on Untrusted Clients .....	96
<i>Guenter Starnberger, Lorenz Frohofer, and Karl M. Goeschka</i>	
A Semi-Markov Survivability Evaluation Model for Intrusion Tolerant Database Systems .....	104
<i>Alex Hai Wang, Su Yan, and Peng Liu</i>	

## Availability and Reliability II

FaT2D: Fault Tolerant Directed Diffusion for Wireless Sensor Networks .....	112
<i>Fatima Zohra Benhamida and Yacine Challal</i>	
An Adaptive Redundancy Oriented Method to Tolerate Soft Errors in SRAM-Based FPGAs Using Unused Resources .....	119
<i>Somayeh Bahramnejad and Hamid Reza Zarandi</i>	
Analysis of Transient Faults on a MIPS-Based Dual-Core Processor .....	125
<i>Iman Faraji, Moslem Didehban, and Hamid Reza Zarandi</i>	

## Risk and Security Management I

Visualizing Past Personal Data Disclosures .....	131
<i>Jan Kolter, Michael Netter, and Günther Pernul</i>	
Strategies for Reducing Risks of Inconsistencies in Access Control Policies .....	140
<i>Bernard Stepien, Stan Matwin, and Amy Felty</i>	
Multi-dimensional Uncertainty Analysis in Secure and Dependable Domain .....	148
<i>Yudistira Asnar and Paolo Giorgini</i>	

## Risk and Security Management II

Information Flow in Disaster Management Systems .....	156
<i>Achim D. Brucker and Dieter Hutter</i>	
Formal Specification and Analysis of an E-voting System .....	164
<i>Komminist Weldemariam, Richard A. Kemmerer, and Adolfo Villafiorita</i>	
Towards a Privacy-Enhanced Social Networking Site .....	172
<i>Esma Aïmeur, Sébastien Gams, and Ai Ho</i>	

## Risk and Security Management III

A Formal Approach Towards Risk-Aware Service Level Analysis and Planning .....	180
<i>Stefan Jakoubi, Simon Tjoa, Sigrun Goluch, and Gerhard Kitzler</i>	
Threat- and Risk-Analysis During Early Security Requirements Engineering .....	188
<i>Holger Schmidt</i>	
An Analysis of Information Security Awareness within Home and Work Environments .....	196
<i>Shuhaili Talib, Nathan L. Clarke, and Steven M. Furnell</i>	

## **ARES 2010 Short Papers**

### **Security and Privacy**

Trust Based Multi Path DSR Protocol .....	204
<i>Poonam Gera, Kumkum Garg, and Manoj Misra</i>	
Enhanced Chaotic Stream Cipher for WSNs .....	210
<i>Rui Miguel Soares Silva, Rui Gustavo Nunes Pereira Crespo, and Mário Serafim dos Santos Nunes</i>	
Zone Based Systems Design Framework for the Realisation of Efficient Block Cipher Based Message Authentication Code Algorithms .....	216
<i>A.A. Adekunle and S.R. Woodhead</i>	

### **Identity Management, Authentication, and Authorization**

A Semantic Security Architecture for Web Services—The Access-eGov Solution .....	222
<i>Stefan Dürbeck, Christoph Fritsch, Günther Pernul, and Rolf Schillinger</i>	
FedWare: Middleware Services to Cope with Information Consistency in Federated Identity Management .....	228
<i>Thorsten Hoellrigl, Jochen Dinger, and Hannes Hartenstein</i>	
Owner-Based Role-Based Access Control OB-RBAC .....	236
<i>Mohsen Saffarian and Babak Sadighi</i>	

### **Cryptography and Secure Protocols**

Program Obfuscation by Strong Cryptography .....	242
<i>Željko Vrba, Pål Halvorsen, and Carsten Griwodz</i>	
Pitfalls in Formal Reasoning about Security Protocols .....	248
<i>Nina Moebius, Kurt Stenzel, and Wolfgang Reif</i>	
Secure Group Communication Using Fractional Public Keys .....	254
<i>Sigurd Eskeland and Vladimir Oleshchuk</i>	

### **Risk and Security Management**

Extending the Gordon and Loeb Model for Information Security Investment .....	258
<i>Jan Willemson</i>	
Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures .....	262
<i>Jocelyn Aubert, Thomas Schaberreiter, Christophe Incou, Djamel Khadraoui, and Benjamin Gâteau</i>	
Planning Dynamic Activity and Resource Allocations Using a Risk-Aware Business Process Management Approach .....	268
<i>Simon Tjoa, Stefan Jakoubi, Sigrun Goluch, and Gerhard Kitzler</i>	

## Miscellaneous

Security and Usability: Analysis and Evaluation .....	275
<i>Ronald Kainda, Ivan Fléchais, and A.W. Roscoe</i>	
Recovery of Skype Application Activity Data from Physical Memory .....	283
<i>Matthew Simon and Jill Slay</i>	
Rejuvenating High Available Virtualized Systems .....	289
<i>Arash Rezaei and Mohsen Sharifi</i>	

## Fifth International Workshop on Frontiers in Availability, Reliability, and Security (FARES 2010 )

### Fraud and Misuse Detection

Detection of Spyware by Mining Executable Files .....	295
<i>Raja Khurram Shahzad, Syed Imran Haider, and Niklas Lavesson</i>	
A Probabilistic Approach for On-Line Sum-Auditing .....	303
<i>Gerardo Canfora and Bice Cavallo</i>	
Towards an Ontology-Based Solution for Managing License Agreement Using Semantic Desktop .....	309
<i>Mansoor Ahmed, Amin Anjomshooa, Muhammad Asfandeyar, A. Min Tjoa, and Abid Khan</i>	

### Intrusion Detection

Optimising IDS Sensor Placement .....	315
<i>Hao Chen, John A. Clark, Siraj A. Shaikh, Howard Chivers, and Philip Nobles</i>	
Layered Higher Order N-grams for Hardening Payload Based Anomaly Intrusion Detection .....	321
<i>Neminath Hubballi, Santosh Biswas, and Sukumar Nandi</i>	
Improving Network Intrusion Detection by Means of Domain-Aware Genetic Programming .....	327
<i>Jorge Blasco, Agustín Orfila, and Arturo Ribagorda</i>	

### Privacy and Trust

On the Simulation of a Software Reputation System .....	333
<i>Martin Boldt, Anton Borg, and Bengt Carlsson</i>	
Model-Driven Application-Level Encryption for the Privacy of E-health Data .....	341
<i>Yun Ding and Karsten Klein</i>	
Communal Reputation and Individual Trust (CRIT) in Wireless Sensor Networks .....	347
<i>Tanveer A Zia and Md Zahidul Islam</i>	

## **Global Information Security**

A Multi-stage Methodology for Ensuring Appropriate Security Culture and Governance .....	353
<i>Solange Ghernouti-Hélie, Igli Tashi, and David Simms</i>	
Development of ICT Infrastructure for Local Socio-Economic System in Japan—Another Approach Toward Cybersecurity in the Non-urban Area .....	361
<i>Hiroshi Nagano</i>	
A National Strategy for an Effective Cybersecurity Approach and Culture .....	370
<i>Solange Ghernouti-Hélie</i>	

## **Software Security and Authentication**

Choosing Authentication Techniques in E-procurement System in Serbia .....	374
<i>Miloš Milovanović, Marija Bogičević, Miroslav Lazović, Dejan Simić, and Dušan Starčević</i>	
A Continuous Authentication System Based on User Behavior Analysis .....	380
<i>Ines Brosso, Alessandro La Neve, Graça Bressan, and Wilson Vicente Ruggiero</i>	
Identifying Security Relevant Warnings from Static Code Analysis Tools through Code Tainting .....	386
<i>Dejan Baca</i>	

## **Digital Content Security**

Reselling Digital Content .....	391
<i>Laila El Aïmani and Yona Raekow</i>	
A New DRM Architecture with Strong Enforcement .....	397
<i>Sascha Müller and Stefan Katzenbeisser</i>	
A Secure and Scalable Grid-Based Content Management System .....	404
<i>Benjamin Aziz, Alvaro Arenas, Giovanni Cortese, Bruno Crispo, and Silvio Causeti</i>	
A Design Pattern for Event-Based Processing of Security-Enriched SOAP Messages .....	410
<i>Nils Gruschka, Meiko Jensen, and Luigi Lo Iacono</i>	

## **The Second International Workshop on Organizational Security Aspects (OSA 2010)**

### **Organizational Aspects of Security: Session 1**

Challenging IS and ISM Standardization for Business Benefits .....	416
<i>Juhani Anttila and Jorma Kajava</i>	
Managing the Asset Risk of SMEs .....	422
<i>Luis Enrique Sánchez, Carlos Ruiz, Eduardo Fernández-Medina, and Mario Piattini</i>	

## Organizational Aspects of Security: Session 2

A Generic Metamodel for IT Security—Attack Modeling for Distributed Systems .....	430
<i>André Miede, Nedislav Nedyalkov, Christian Gottron, André König, Nicolas Repp, and Ralf Steinmetz</i>	
Combining Misuse Cases with Attack Trees and Security Activity Models .....	438
<i>Inger Anne Tøndel, Jostein Jensen, and Lillian Røstad</i>	
External Insider Threat: A Real Security Challenge in Enterprise Value Webs .....	446
<i>Virginia N.L. Franqueira, André van Cleeff, Pascal van Eck, and Roel Wieringa</i>	

## Organizational Aspects of Security: Session 3

Secure Monitoring of Service Level Agreements .....	454
<i>K.P. Clark, M.E. Warnier, F.M.T. Brazier, and T.B. Quillinan</i>	
Fighting Phishing with Trusted Email .....	462
<i>Jordan Crain, Lukasz Opyrchal, and Atul Prakash</i>	
Application and Economic Implications of an Automated Requirement-Oriented and Standard-Based Compliance Monitoring and Reporting Prototype .....	468
<i>Matthias Kehlenbeck, Thorben Sandner, and Michael H. Breitner</i>	

## Organizational Aspects of Security: Session 4

A Taxonomy Refining the Security Requirements for Electronic Voting: Analyzing Helios as a Proof of Concept .....	475
<i>Lucie Langer, Axel Schmidt, Johannes Buchmann, and Melanie Volkamer</i>	
Secured Key Distribution Scheme for Cryptographic Key Management System .....	481
<i>Kyawt Kyawt Khaing and Khin Mi Mi Aung</i>	
One Size Fits None: The Importance of Detector Parameterization .....	487
<i>Natasha Bodorik and A. Nur Zincir-Heywood</i>	

## Fourth International Workshop on Secure Software Engineering (SecSE 2010 )

### Agile Development and Hot Patching

Supporting Authorization Policy Modification in Agile Development of Web Applications .....	495
<i>Steffen Bartsch</i>	
The Road to Hell is Paved with Good Intentions: A Story of (In)secure Software Development .....	501
<i>Richard Sasson, Martin Gilje Jaatun, and Jostein Jensen</i>	
Katana: A Hot Patching Framework for ELF Executables .....	507
<i>Ashwin Ramaswamy, Sergej Bratus, Sean W. Smith, and Michael E. Locasto</i>	



## Testing, Monitoring, and Validation

Investigating the Limitations of Java Annotations for Input Validation .....	513
<i>Federico Mancini, Dag Hovland, and Khalid A. Mughal</i>	
Classification of Buffer Overflow Vulnerability Monitors .....	519
<i>Hossain Shahriar and Mohammad Zulkernine</i>	
Configuration Fuzzing for Software Vulnerability Detection .....	525
<i>Huning Dai, Christian Murphy, and Gail Kaiser</i>	

## Security Modeling and Vulnerabilities

Practical Experience Gained from Modeling Security Goals: Using SGITs in an Industrial Project .....	531
<i>Christian Jung, Frank Elberzhager, Alessandra Bagnato, and Fabio Raiteri</i>	
Security Modeling and Tool Support Advantages .....	537
<i>Egil Trygve Baadshaug, Gencer Erdogan, and Per Håkon Meland</i>	
Analysing and Visualising Security and Usability in IRIS .....	543
<i>Shamal Faily and Ivan Fléchais</i>	
Security and Performance Aspects of an Agent-Based Link-Layer Vulnerability Discovery Mechanism .....	549
<i>Ziyad S. Al-Salloum and Stephen D. Wolthusen</i>	

## Fourth International Workshop on Secure Systems Methodologies Using Patterns (SPattern 2010 )

### SPattern Application

Model-Driven Security Patterns Application Based on Dependences among Patterns .....	555
<i>Yuki Shiroma, Hironori Washizaki, Yoshiaki Fukazawa, Atsuto Kubo, and Nobukazu Yoshioka</i>	
Refining the Pattern-Based Reference Model for Electronic Invoices by Incorporating Threats .....	560
<i>Michael Netter, Eduardo B. Fernandez, and Günther Pernul</i>	
Measuring the Level of Security Introduced by Security Patterns .....	565
<i>Eduardo B. Fernandez, Nobukazu Yoshioka, Hironori Washizaki, and Michael VanHilst</i>	

### SPattern Development

Patterns for Secure Boot and Secure Storage in Computer Systems .....	569
<i>Hans Löhr, Ahmad-Reza Sadeghi, and Marcel Winandy</i>	

## Fourth International Workshop on Advances in Information Security (WAIS 2010)

### Identity and Privacy

A Consideration of the Reliability of Registration and Attribute Exchange .....	574
<i>Yoshio Kakizaki and Keiichi Iwamura</i>	
Binomial-Mix-Based Location Anonymizer System with Global Dummy Generation to Preserve User Location Privacy in Location-Based Services .....	580
<i>Minh-Triet Tran, Isao Echizen, and Anh-Duc Duong</i>	
Multiple Designated Verifiers Signatures Reconsidered .....	586
<i>Mebae Ushida, Tetsuya Izu, Masahiko Takenaka, and Kazuo Ohta</i>	

### System Security

LSM-Based Secure System Monitoring Using Kernel Protection Schemes .....	591
<i>Takamasa Isohara, Keisuke Takemori, Yutaka Miyake, Ning Qu, and Adrian Perrig</i>	
Formalization of Viruses and Malware Through Process Algebras .....	597
<i>Grégoire Jacob, Eric Filiol, and Hervé Debar</i>	
Heuristics for Detecting Botnet Coordinated Attacks .....	603
<i>Kazuya Kuwabara, Hiroaki Kikuchi, Masato Terada, and Masashi Fujiwara</i>	

### Experimental and Physical Security

An Improvement of Robustness Against Physical Attacks and Equipment Independence in Information Hiding Based on the Artificial Fiber Pattern .....	608
<i>Kitahiro Kaneda, Yuki Fujii, Keiichi Iwamura, and Seiichiro Hangai</i>	
Large Scale Demonstration Experiments Towards Achieving Practical Traceback on the Internet .....	613
<i>Ken Wakasa, Hiroaki Hazeyama, Toshifumi Kai, Akira Hashiguchi, Masaya Yamagata, Masahiko Fujinaga, Ryunosuke Ohshima, and Takashi Shintani</i>	
Quantum Detection of Wavelength Division Multiplexing Optical Coherent Signals in Lossy Channels .....	619
<i>Atsushi Waseda, Masahide Sasaki, Masahiro Takeoka, Mikio Fujiwara, Morio Toyoshima, and Hidema Tanaka</i>	
Experimental Results on Cheon's Algorithm .....	625
<i>Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda</i>	

## Third International Workshop on Digital Forensics (WSDF 2010)

### Digital Forensic Workshop: Session 1

The 'Explore, Investigate and Correlate' (EIC) Conceptual Framework for Digital Forensics Information Visualisation .....	629
<i>Grant Osborne, Benjamin Turnbull, and Jill Slay</i>	
A Model for Computer Profiling .....	635
<i>Andrew Marrington, George Mohay, Hasumukh Morarji, and Andrew Clark</i>	

Using Normalized Compression Distance for Classifying File Fragments .....	641
<i>Stefan Axelsson</i>	

## **Digital Forensic Workshop: Session 2**

A Multi-component View of Digital Forensics .....	647
<i>C.P. Grobler, C.P. Louwrens, and S.H. von Solms</i>	
Blind Steganalysis: A Countermeasure for Binary Image Steganography .....	653
<i>Kang Leng Chiew and Josef Pieprzyk</i>	
Log Analysis Towards an Automated Forensic Diagnosis System .....	659
<i>Jorge Herrerías and Roberto Gómez</i>	

## **Digital Forensic Workshop: Session 3**

A Function Oriented Methodology to Validate and Verify Forensic Copy Function of Digital Forensic Tools .....	665
<i>Yinghua Guo and Jill Slay</i>	
A Complexity Based Model for Quantifying Forensic Evidential Probabilities .....	671
<i>Richard E. Overill, Jantje A.M. Silomon, and Kam-Pui Chow</i>	
A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations .....	677
<i>C.P. Grobler, C.P. Louwrens, and S.H. von Solms</i>	
Estimating Hidden Message Length in Binary Image Embedded by Using Boundary Pixels Steganography .....	683
<i>Kang Leng Chiew and Josef Pieprzyk</i>	

## **Digital Forensic Workshop Session 4**

Information Flow Control Using the Java Virtual Machine Tool Interface (JVMTI) .....	689
<i>Jason Howarth, Irfan Altas, and Barney Dalgarno</i>	
A Prototype for Support of Computer Forensic Analysis Combined with the Expected Knowledge Level of an Attacker to More Efficiently Achieve Investigation Results .....	696
<i>Maximilian Bielecki and Gerald Quirchmayr</i>	
A Novel Image Hiding Scheme Using Content Aware Seam Carving Method .....	702
<i>Zahra Toony and Mansour Jamzad</i>	

## **Author Index**