2011 Sixth International Conference on Availability, Reliability and Security

(ARES 2011)

Vienna, Austria
22 – 26 August 2011

IEEE Catalog Number:	CFP1139A-PRT
ISBN:	978-1-4577-0979-1

2011 Sixth International Conference on Availability, Reliability and Security

ARES 2011

Table of Contents

Message from the ARES 2011 General Co-Chairs, Program Committee Co-Chairs, and Keynote Chairs.........xv

Message from the ARES 2011 Workshop Co-Chairs.........xvii

Message from the FARES 2011 Workshop Co-chairs.........xviii

Message from the DYADEM-FTS 2011 Workshop Organizers.........xix

Message from the PBD 2011 Workshop Organizers.........xx

Message from the RISI 2011 Workshop Organizers.........xxi

Message from the SAPAIS 2011 Workshop Organizers.........xxii

Message from the SECSE 2011 Workshop Organizers.........xxiii

Message from the WSDF 2011 Workshop Organizers.........xxiv

Message from the OSA 2011 Workshop Organizers.........xxv

The Sixth International Conference on Availability, Reliability and Security (ARES 2011)

ARES F1 – Access Control

An Approach to Access Control under Uncertainty.........1
Farzad Salim, Jason Reid, Ed Dawson, and Uwe Dulleck

Support Access to Distributed EPRs with Three Levels of Identity Privacy Preservation.........9
Rima Addas and Ning Zhang

Smatch Model: Extending RBAC Sessions in Virtualization Environment.........17
Nora Cuppens-Boulahia, Frédéric Cuppens, and Marie Nuadi

ARES F2 - Identity Management and Access Control

AW-RBAC: Access Control in Adaptive Workflow Systems.........27
Maria Leitner, Stefanie Rinderle-Ma, and Jürgen Mangler

The Role Mining Process Model - Underlining the Need for a Comprehensive Research Perspective.........35
Ludwig Fuchs and Stefan Meier

Biometric Authentication as a Service for Enterprise Identity Management Deployment: A Data Protection Perspective 43
Christian Senk and Florian Dotzler

ARES F3 – Software

An Obfuscation-Based Approach against Injection Attacks 51
Fabrizio Baiardi and Daniele Sgandurra

Using CVSS in Attack Graphs 59
Laurent Gallon and Jean Jacques Bascou

Selecting Software Packages for Secure Database Installations 67
Afonso Araújo Neto and Marco Vieira

ARES F4 – Dependable Systems

Probabilistic Fault-tolerance of Distributed Services: A Paradigm for Dependable Applications 75
Kaliappa Ravindran

Proactive Failure Management by Integrated Unsupervised and Semi-Supervised Learning for Dependable Cloud Systems 83
Qiang Guan, Ziming Zhang, and Song Fu

ARES F5 – Cryptography

A Novel Phase Coding Technique for Steganography in Auditive Media 91
Marcus Nutzinger and Jüergen Wurzer

ESPOON: Enforcing Encrypted Security Policies in Outsourced Environments 99
Muhammad Rizwan Asghar, Mihaela Ion, Giovanni Russello, and Bruno Crispo

A Robust Anti-tamper Protection Scheme 109
Hing-Chung Tsang, Moon-Chuen Lee, and Chi-Man Pun

ARES F6 – Cryptography & Electronic Voting

Formalization of Receipt-Freeness in the Context of Electronic Voting 119
Katharina Braunlich and Rüdiger Grimm

Introducing Verifiability in the POLYAS Remote Electronic Voting System 127
Maina M. Olembo, Patrick Schmidt, and Melanie Volkamer

Non-Parallelizable and Non-Interactive Client Puzzles from Modular Square Roots 135
Yves Igor Jerschow and Martin Mauve

ARES F7 – Network and Data Security

Declassification Policy Management in Dynamic Information Systems 143
Julien A. Thomas, Nora Cuppens-Boulahia, and Frédéric Cuppens

ASPF: Adaptive anti-SPIT Policy-based Framework 153
Yannis Soupionis and Dimitris Gritzalis

Modeling and Analyzing Server System with Rejuvenation through SysML and Stochastic Reward Nets 161
Ermeson C. Andrade, Fumio Machida, Dong-Seong Kim, and Kishor S. Trivedi

The Sixth International Conference on Availability, Reliability and Security - Short Papers (ARES Short 2011)

ARES S1 – Network and Software Security 1

Early Detection of Security Misconfiguration Vulnerabilities in Web Applications 169
Birhanu Eshete, Adolfo Villafiorita, and Komminist Weldemariam

Implicit Buffer Overflow Protection Using Memory Segregation 175
Brent G. Roth and Eugene H. Spafford

Recovery of Pidgin Chat Communication Artefacts from Physical Memory: A Pilot Test to Determine Feasibility 183
Matthew Phillip Simon and Jill Slay

ARES S2 – Network and Software Security 2

Accurate Adware Detection Using Opcode Sequence Extraction 189
Raja Khurram Shahzad, Niklas Lavesson, and Henric Johnson

Digital Forensics Infovis: An Implementation of a Process for Visualisation of Digital Evidence 196
Grant Osborne and Jill Slay

Security SLAs for Federated Cloud Services 202
Karin Bernsmed, Martin Gilje Jaatun, Per Håkon Meland, and Astrid Undheim

ARES S3 – Network and Software Security 3

Parametric Differences between a Real-world Distributed Denial-of-Service Attack and a Flash Event 210
Sajal Bhatia, George Mohay, Alan Tickle, and Ejaz Ahmed

Observer-based Testing of Distributed Protocols Designed for Harsh Environments 218
Kaliappa Ravindran and Gwangyu Ding

Trustworthiness Benchmarking of Web Applications Using Static Code Analysis 224
Afonso Araújo Neto and Marco Vieira

ARES S4 - Access Control & Security Modeling 1

A Trustworthy Usage Control Enforcement Framework 230
Ricardo Neisse, Alexander Pretschner, and Valentina Di Giacomo

An Attribute Based Framework for Risk-Adaptive Access Control Models 236
Savith Kandala, Ravi Sandhu, and Venkata Bhamidipati

ACON: Activity-Centric Access Control for Social Computing 242
Jaehong Park, Ravi Sandhu, and Yuan Cheng

ARES S5 - Access Control & Security Modeling 2

Dynamic Responsibilities Assignment in Critical Electronic Institutions - A Context-Aware Solution for in Crisis Access Right Management 248
Cédric Bonhomme, Christophe Feltus, and Michaël Petit

A Hypervisor-Based Bus System for Usage Control 254
Cornelius Moucha, Enrico Lovat, and Alexander Pretschner

An Approach to Model-based Development of Secure and Reliable Systems 260
Eduardo B. Fernandez, Hironori Washizaki, Nobukazu Yoshioka, and Michael VanHilst

ARES S6 - Access Control & Security Modeling 3

Techniques for Automating Policy Specification for Application-oriented Access Controls 266
Z. Cliffe Schreuders, Christian Payne, and Tanya McGill

Model-Based Security Verification and Testing for Smart-cards 272
Elizabeta Fourneret, Martín Ochoa, Fabrice Bouquet, Julien Botella, Jan Jürjens, and Parvaneh Yousefi

Information Security Automation: How Far Can We Go? 280
Raydel Montesino and Stefan Fenz

ARES S7 – Theory

An Epistemic Logic Based Framework for Reasoning about Information Hiding 286
I. Goriac

Bulletin Boards in Voting Systems: Modelling and Measuring Privacy 294
Hugo Jonker and Jun Pang

System State Discovery Via Information Content Clustering of System Logs 301
Adetokunbo Makanju, A. Nur Zincir-Heywood, and Evangelos E. Milios

File Block Classification by Support Vector Machine 307
Luigi Sportiello and Stefano Zanero

ARES S8 – Organizational Security

Security and Privacy in Companies: State-of-the-art and Qualitative Analysis 313
Barbara Krumay and Marie Caroline Oetzel

Hidden Price of User Authentication: Cost Analysis and Stakeholder Motivation 321
Ludwig Meyer, Martin Auer, Markus Klemen, and Stefan Biffl

Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing 327
Kristian Beckers, Holger Schmidt, Jan-Christoph Küster, and Stephan Faßbender

Responsibility-driven Design and Development of Process-aware Security Policies 334
Maria Leitner, Stefanie Rinderle-Ma, and Juergen Mangler

ARES S9 – Cryptography

Fast Implementation of the Advanced Encryption Standard Using Atmega1281 342
Kasumi Toriumi, Yoshio Kakizaki, and Keiichi Iwamura

Optimization of Privacy Preserving Mechanisms in Homogeneous Collaborative Association Rules Mining 347
Marcin Gorawski and Zacheusz Siedlecki

CDRAS: An Approach to Dealing with Man-in-the-Middle Attacks in the Context of Voice over IP 353
Stefan Hofbauer, Gerald Quirchmayr, and Christopher C. Wills

Crowds Based on Secret-Sharing 359
Stefan Rass, Raphael Wigoutschnigg, and Peter Schartner

ARES S10 – Dependability

A Gate Level Analysis of Transient Faults Effects on Dual-Core Chip-Multi Processors 365
Moslem Didehban, Ario Sadafi, Sajjad Salehi, and Mohammad Bagher Chami

Secure Broadcast with One-Time Signatures in Controller Area Networks 371
Bogdan Groza and Stefan Murvay

Performance Evaluation of ID-based Group Key Agreement Protocols 377
Elisavet Konstantinou, Eleni Klaoudatou, and Pavlos Kamparmpakis

ARES Industrial Track (Industrial Track)

Industrial Track 1

Preliminary Thoughts on Cost-based Investment Decisions in IT: A Problem Analysis 385
Ralf Gitzel, Christian Cuske, and Carsten Münch

On the Context-aware, Personalized Delivery of Process Information: Viewpoints, Problems, and Requirements 390
Markus Hipp, Bela Mutschler, and Manfred Reichert

Industrial Track 2

Study of Countermeasures for Content Leaks by Video Recording 398
Masaki Fujikawa, Junki Akimoto, Fumihiko Oda, Kengo Moriyasu, Shingo Fuchi, and Yoshikazu Takeda

Product Line Engineering in Large-Scale Lean and Agile Software Product Development Environments - Towards a Hybrid Approach to Decentral Control and Managed Reuse 404
Benjamin Blau and Tobias Hildenbrand

Seamless Fusion of Secure Software and Trusted USB Token for Protecting Enterprise & Government Data 409
Asad M. Ali

Dynamic Aspects in Dependability Models for Fault-Tolerant Systems (DYADEM-FTS 2011)

DYADEM-FTS 1

Considering Dependent Components in the Terminal Pair Reliability Problem 415
Minh Lê and Max Walter

Cyber-Physical Systems Based Modeling of Dependability of Complex Network Systems 423
Kaliappa Ravindran

Compositional Synthesis of Temporal Fault Trees from State Machines 429
Nidhal Mahmud, Martin Walker, and Yiannis Papadopoulos

Stepwise Refinement of Complex Dependability Models Using LARES+ 436
Max Walter

Sixth International Workshop on Frontiers in Availability, Reliability and Security (FARES 2011)

Software, Network Security and Cryptography 1

Privacy Frost: A User-Oriented Data Anonymization Tool 442
Shinsaku Kiyomoto, Yutaka Miyake, and Toshiaki Tanaka

Key Management Scheme Applicable to Various Topologies of Sensor Networks 448
Hidetoshi Yukimaru, Yoshio Kakizaki, and Keiichi Iwamura

An Inductive Approach to Provable Anonymity 454
Yongjian Li and Jun Pang

Software, Network Security and Cryptography 2

Information Security for Service Oriented Computing: Ally or Antagonist 460
Jacqui Chetty and Marijke Coetzee

Van Wijngaarden Grammars and Metamorphism 466
Gueguen Geoffroy

PUF Based Scalable Private RFID Authentication 473
Mete Akgün and M. Ufuk Çağlayan

Software, Network Security and Cryptography 3

Practitioners' Perspectives on Security in Agile Development 479
Steffen Bartsch

Security Issues in a Synchronous e-Training Platform 485
Juan C. Granda, Pelayo Nuño, Daniel F. García, and Francisco J. Suárez

Some Security Issues in SCALANCE Wireless Industrial Networks 493
Marius Cristea, Bogdan Groza, and Mihai Iacob

Software Security 1

Development and Trial Application of Prototype Program for "Social-MRC": Social Consensus Formation Support System Concerning IT Risk Countermeasures 499
Ryoichi Sasaki, Kazushige Takakusaki, Masaru Ohkawara, Hiroshi Yajima, Hidetaka Masuda, and Tetsuro Kobayashi

Experimental Comparison of Misuse Case Maps with Misuse Cases and System Architecture Diagrams for Eliciting Security Vulnerabilities and Mitigations 507
Peter Karpati, Andreas L. Opdahl, and Guttorm Sindre

Proactive Detection of Kernel-Mode Rootkits 515
Pablo Bravo and Daniel F. Garcia

Software Security 2

Service Security Requirement Profiles for Telecom: How Software Engineers May Tackle Security 521
Albin Zuccato, Nils Daniels, and Cheeverat Jampathom

Effective Security Impact Analysis with Patterns for Software Enhancement 527
Takao Okubo, Haruhiko Kaiya, and Nobukazu Yoshioka

Web Services Security Policy Assertion Trade-offs 535
Tristan Lavarack and Marijke Coetzee

Software Security and Access Control

Federated Authentication and Authorisation in the Social Science Domain 541
John Watt, Richard O. Sinnott, George Inman, and David Chadwick

A Proposed Web Access Control System Request Policy Framework for Cooperation of DNS and a Web Browser 549
Takashi Uemura, Shota Takagi, Yusuke Kosuda, and Ryoichi Sasaki

An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and Other Delights 555
Mikael Ates, Serge Ravet, Abakar Mohamat Ahmat, and Jacques Fayolle

Attacks and Security Modeling

Wormhole Attacks Mitigation in Ad Hoc Networks 561
Mariannne A. Azer

A Distributed Intrusion Detection Model Based on a Society of Intelligent Mobile Agents for Ad Hoc Network 569
Ghenima Bourkache, Mohamed Mezghiche, and Karim Tamine

The Limes Security Model for Information Flow Control 573
Eckehard Hermann

Tag Impersonation Attack on Two RFID Mutual Authentication Protocols 581
Masoumeh Safkhani, Nasour Bagheri, Majid Naderi, Yiyuan Luo, and Qi Chai

The Third International Workshop on Organizational Security Aspects (OSA 2011)

Information Security Integral Engineering Technique and its Application in ISMS Design 585
Alexander Lyubimov, Dmitry Cheremushkin, Natalia Andreeva, and Sergey Shustikov

Optimal Budget Allocation in Budget-based Access Control 591
Farzad Salim, Uwe Dulleck, Jason Reid, and Ed Dawson

A Study of Prevention for Social Engineering Attacks Using Real/Fake Organization's Uniforms: Application of Radio and Intra-Body Communication Technologies 597
Masaki Fujikawa and Masakatsu Nishigaki

First International Workshop on Privacy by Design (PBD 2011)

Session 1

LiDSec- A Lightweight Pseudonymization Approach for Privacy-Preserving Publishing of Textual Personal Information 603
Reza Rawassizadeh, Johannes Heurix, Soheil Khosravipour, and A. Min Tjoa

A Server-side Approach to Privacy Policy Matching 609
Åsmund Ahlmann Nyre, Karin Bernsmed, Solvår Bø, and Stian Pedersen

Enhance Data Privacy in Service Compositions through a Privacy Proxy 615
Zhendong Ma, Jürgen Manglery, Christian Wagner, and Thomas Bleier

Session 2

Learning Privacy Preferences 621
Inger Anne Tøndel, Åsmund Ahlmann Nyre, and Karin Bernsmed

Privacy Verification Using Ontologies 627
Martin Kost, Johann-Christoph Freytag, Frank Kargl, and Antonio Kung

A Survey on Saving Personal Data in the Mobile Phone 633
Iosif Androulidakis and Gorazd Kandus

Workshop on Resilience and IT-Risk in Social Infrastructures (RISI 2011)

Session 1

Gaining Flexibility and Compliance in Rescue Processes with BPM 639
Kai Kittel and Stefan Sackmann

Using Generalization Patterns for Fingerprinting Sets of Partially Anonymized Microdata in the Course of Disasters 645
Sebastian Schrittwieser, Peter Kieseberg, Isao Echizen, Sven Wohlgemuth, and Noboru Sonehara

Improving Resilience with Community Cloud Computing 650
Gerard Garlick

Session 2

A Visualization Method for Helping Children Assess the Risk of Websites 656
Tomoko Kajiyama

Testbed for Mobile Telephony Networks 661
Konrad Meier, Dennis Wehrle, Klaus Rechert, and Dirk von Suchodoletz

International Workshop on Security Aspects of Process-aware Information Systems (SAPAIS 2011)

Deriving Current State RBAC Models from Event Logs 667
Anne Baumgrass

Integrity and Confidentiality Annotations for Service Interfaces in SoaML Models 673
Bernhard Hoisl and Stefan Sobernig

Consistency Checks for Duties in Extended UML2 Activity Models 680
Sigrid Schefer

Security Policies in Adaptive Process-Aware Information Systems: Existing Approaches and Challenges 686
Maria Leitner

SWAT: A Security Workflow Analysis Toolkit for Reliably Secure Process-aware Information Systems 692
Rafael Accorsi, Claus Wonnemann, and Sebastian Dochow

Fifth International Workshop on Secure Software Engineering (SecSE 2011)

SecSE 1

Security Evaluation of Service-oriented Systems with an Extensible Knowledge Base 698
Christian Jung, Manuel Rudolph, and Reinhard Schwarz

Security in Model Driven Development: A Survey 704
Jostein Jensen and Martin Gilje Jaatun

Characterising and Analysing Security Requirements Modelling Initiatives 710
Peter Karpati, Guttorm Sindre, and Andreas L. Opdahl

SecSE 2

User-Centered Information Security Policy Development in a Post-Stuxnet World 716
Shamal Faily and Ivan Fléchais

Here's Johnny: A Methodology for Developing Attacker Personas 722
Andrea Atzeni, Cesare Cameroni, Shamal Faily, John Lyle, and Ivan Flechais

Enhancing Fuzzing Technique for OKL4 Syscalls Testing 728
Amaury Gauthier, Clément Mazin, Julien Iguchi-Cartigny, and Jean-Louis Lanet

SecSE 3

Evaluating RBAC Supported Techniques and their Validation and Verification 734
Nafees Qamar, Yves Ledru, and Akram Idani

Optimising CAPTCHA Generation 740
Suliman A. Alsuhibany

The Java SPI Framework for Security Protocol Implementation 746
Matteo Avalle, Alfredo Pironti, Riccardo Sisto, and Davide Pozza

The Fourth International Workshop on Digital Forensics (WSDF 2011)

Roadmap to Approaches for Carving of Fragmented Multimedia Files 752
Rainer Poisel and Simon Tjoa

A Discussion of Visualization Techniques for the Analysis of Digital Evidence 758
Gerald Schrenk and Rainer Poisel

A Complexity Based Forensic Analysis of the Trojan Horse Defence 764
Richard E. Overill and Jantje A.M. Silomon

Author Index 769