

2014 Ninth International Conference on Availability, Reliability and Security

(ARES 2014)

**Fribourg, Switzerland
8-12 September 2014**



**IEEE Catalog Number: CFP1439A-POD
ISBN: 978-1-4799-7876-2**

2014 9th International Conference on Availability, Reliability and Security

ARES 2014 Table of Contents

Welcome Message from ARES Program Committee	
Co-Chairs and General Chair	xii
ARES 2014 Organizing Committee	xiii
Welcome Message from ARES Workshop Chair	xvi
Welcome Message from the ARES-IND 2014 Workshop	
Organizers	xvii
ARES-IND 2014 Workshop Program Committee	xviii
Welcome Message from the FARES 2014 Workshop	
Organizers	xix
Welcome Message from the ECTCM 2014 Workshop	
Organizers	xx
ECTCM 2014 Workshop Program Committee	xxi
Welcome Message from the IWSMA 2014 Workshop	
Organizers	xxii
IWSMA 2014 Workshop Program Committee	xxiii
Welcome Message from the RAMSS 2014 Workshop	
Organizers	xxiv
RAMSS 2014 Workshop Program Committee	xxv
Welcome Message from the RISI 2014 Workshop	
Organizers	xxvi
RISI 2014 Workshop Program Committee	xxviii
Welcome Message from the SAW 2014 Workshop	
Organizers	xxix
SAW 2014 Workshop Program Committee	xxx
Welcome Message from the SecATM 2014 Workshop	
Organizers	xxxi
SecATM 2014 Workshop Program Committee	xxxii
Welcome Message from the WSDF 2014 Workshop	
Organizers	xxxiii
WSDF 2014 Workshop Program Committee	xxxiv

ARES Conference 2014 Program: Full Papers

ARES Full I: Best Paper Session

A New Access Control Scheme for Facebook-Style Social Networks	1
<i>Jun Pang and Yang Zhang</i>	
No Smurfs: Revealing Fraud Chains in Mobile Money Transfers	11
<i>Maria Zhdanova, Jürgen Repp, Roland Rieke, Chrystel Gaber, and Baptiste Hemery</i>	
BitTorrent Sync: Network Investigation Methodology	21
<i>Mark Scanlon, Jason Farina, and M-Tahar Kechadi</i>	

ARES Full II: Mobile Security and Attack Prevention

Divide-and-Conquer: Why Android Malware Cannot Be Stopped	30
<i>Dominik Maier, Tilo Müller, and Mykola Protsenko</i>	
DroidForce: Enforcing Complex, Data-centric, System-wide Policies in Android	40
<i>Siegfried Rasthofer, Steven Arzt, Enrico Lovat, and Eric Bodden</i>	
Lobotomy: An Architecture for JIT Spraying Mitigation	50
<i>Martin Jauernig, Matthias Neugschwandtner, Christian Platzer, and Paolo Milani Comparetti</i>	

ARES Full III: Secure Protocols

A Formal Model and Analysis of the MQ Telemetry Transport Protocol	59
<i>Benjamin Aziz</i>	
Practical Attack on Bilinear Pairings to Disclose the Secrets of Embedded Devices	69
<i>Thomas Unterluggauer and Erich Wenger</i>	
A Model-Based Security Toolkit for the Internet of Things	78
<i>Ricardo Neisse, Igor Nai Fovino, Gianmarco Baldini, Vera Stavroulaki, Panagiotis Vlachas, and Raffaele Giaffreda</i>	

ARES Full IV: Trust and Availability

Rethread: A Low-Cost Transient Fault Recovery Scheme for Multithreaded Processors	88
<i>Jian Fu, Qiang Yang, Raphael Poss, Chris R. Jesshope, and Chunyuan Zhang</i>	
Visualizing Transaction Context in Trust and Reputation Systems	94
<i>Johannes Säger and Günther Pernul</i>	
Enhanced Configuration Generation Approach for Highly Available COTS Based Systems	104
<i>Parsa Pournali, Ferhat Khendek, and Maria Toeroe</i>	
Phishdentity: Leverage Website Favicon to Offset Polymorphic Phishing Website	114
<i>Jeffrey Choo Soon Fatt, Chiew Kang Leng, and Sze San Nah</i>	

ARES Conference 2014 Program: Short Papers

ARES Short I: Ontologies and Integrated Devices

EM Leakage of RFID Devices—Comparison of Two Measurement Approaches	120
<i>Thomas Korak and Thomas Plos</i>	
Supporting Security Automation for Multi-chassis Link Aggregation Groups via the Interconnected-Asset Ontology	126
<i>Henk Birkholz and Ingo Sieverdingbeck</i>	
Concurrent Queries in Location Based Services	134
<i>Emad Elabd and Mohand-Said Hacid</i>	

ARES Short II: Security and Privacy

Palpable Privacy through Declarative Information Flows Tracking for Smart Buildings	140
<i>François Lesueur, Sabina Surdu, Romuald Thion, Yann Gripay, and Meriam Ben Ghorbel-Talbi</i>	
An Enhanced Linkable Anonymous Access Protocol of the Distributed Electronic Patient Records	146
<i>Rima Addas and Ning Zhang</i>	
Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy	152
<i>Christian Zimmermann, Rafael Accorsi, and Günter Müller</i>	
Healthcare Services in the Cloud—Obstacles to Adoption, and a Way Forward	158
<i>Karin Bernsmed, Daniela Soares Cruzes, Martin Gilje Jaatun, Børge Haugset, and Erlend Andreas Gjære</i>	

ARES Short III: Software Security and Authentication

Continuous and Non-intrusive Reauthentication of Web Sessions Based on Mouse Dynamics	166
<i>Eric Medvet, Alberto Bartoli, Francesca Boem, and Fabiano Tarlao</i>	
What Does the Fox Say? On the Security Architecture of Firefox OS	172
<i>Marta Piekarska, Bhargava Shastry, and Ravishankar Borgaonkar</i>	
Verifying Implementation of Security Design Patterns Using a Test Template	178
<i>Masatoshi Yoshizawa, Takanori Kobashi, Hironori Washizaki, Yoshiaki Fukazawa, Takao Okubo, Haruhiko Kaiya, and Nobukazu Yoshioka</i>	
AES-SEC: Improving Software Obfuscation through Hardware-Assistance	184
<i>Sebastian Schrittwieser, Stefan Katzenbeisser, Georg Merzdovnik, Peter Kieseberg, and Edgar Weippl</i>	

ARES Industrial Track

Fighting Botnets with Cyber-Security Analytics: Dealing with Heterogeneous Cyber-Security Information in New Generation SIEMs	192
<i>Beatriz Gallego-Nicasio Crespo and Alan Garwood</i>	
Network Security Analysis Using Behavior History Graph	199
<i>Mirko Sailio, Matti Mantere, and Sami Noponen</i>	

The Ninth International Workshop on Frontiers in Availability, Reliability, and Security (FARES 2014)

A Usable Android Application Implementing Distributed Cryptography for Election Authorities	207
<i>Stephan Neumann, Oksana Kulyk, and Melanie Volkamer</i>	
Complete SIP Message Obfuscation: PrivaSIP over Tor	217
<i>Georgios Karopoulos, Alexandros Fakis, and Georgios Kambourakis</i>	
Privacy Preservation in Location-Based Mobile Applications: Research Directions	227
<i>Asma Patel and Esther Palomar</i>	
Challenges of Composing XACML Policies	234
<i>Bernard Stepien, Amy Felty, and Stan Matwin</i>	
EmailCloak: A Practical and Flexible Approach to Improve Email Privacy	242
<i>Italo Dacosta, Andreas Put, and Bart De Decker</i>	
Quality Matters: Systematizing Quality Deficiencies in the Documentation of Business Security Requirements	251
<i>Christian Sillaber and Ruth Breu</i>	
Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A	259
<i>Bahareh Shojaie, Hannes Federrath, and Iman Saberi</i>	
A Proposal for a Unified Identity Card for Use in an Academic Federation Environment	265
<i>Felipe Coral Sasso, Ricardo Alexandre Reinaldo de Moraes, and Jean Everson Martina</i>	
Defining Malicious Behavior	273
<i>Hermann Dornhackl, Konstantin Kadletz, Robert Luh, and Paul Tavalato</i>	

The Second International Workshop on Emerging Cyberthreats and Countermeasures (ECTCM 2014)

The SMM Rootkit Revisited: Fun with USB	279
<i>Joshua Schiffman and David Kaplan</i>	
Towards a Hardware Trojan Detection Cycle	287
<i>Adrian Dabrowski, Heidelinde Hobel, Johanna Ullrich, Katharina Krombholz, and Edgar Weippl</i>	
PhiGARo: Automatic Phishing Detection and Incident Response Framework	295
<i>Martin Husák and Jakub Cegan</i>	
Performance Measures of Behavior-Based Signatures: An Anti-malware Solution for Platforms with Limited Computing Resource	303
<i>Kelly Hughes and Yanzhen Qu</i>	
Network Security Monitoring in a Small-Scale Smart-Grid Laboratory	310
<i>Matti Mantere, Sami Noponen, Pia Olli, and Jarno Salonen</i>	
Increasing the Resilience and Trustworthiness of OpenID Identity Providers for Future Networks and Services	317
<i>Diego Kreutz, Eduardo Feitosa, Hugo Cunha, Heiko Niedermayer, and Holger Kinkel</i>	

The Second International Workshop on Security of Mobile Applications (IWSMA 2014)

A Trust Management Based Security Mechanism against Collusion Attacks in a MANET Environment	325
<i>Aida Ben Chehida Douss, Ryma Abassi, and Sihem Guemara El Fatmi</i>	
A Resource-Optimized Approach to Efficient Early Detection of Mobile Malware	333
<i>Jelena Milosevic, Andreas Dittrich, Alberto Ferrante, and Miroslaw Malek</i>	
An Improved Role-Based Access to Android Applications with JCHR	341
<i>Stefano Bistarelli, Gianpiero Costantino, Fabio Martinelli, and Francesco Santini</i>	
Qualified Electronic Signature via SIM Card Using JavaCard 3 Connected Edition Platform	349
<i>Jakub Breier and Adam Pomothy</i>	

The Second International Workshop on Statistical Methods in Reliability Assessment of Complex Industrial Multi-state Systems (RAMSS 2014)

Analysis of Algorithms for Computation of Direct Partial Logic Derivatives in Multiple-Valued Decision Diagrams	356
<i>Jozef Kostolny, Miroslav Kvassay, and Elena Zaitseva</i>	
Stochastic Model for Medical Image Segmentation	362
<i>Zeev Barzily, Mingyue Ding, and Zeev Volkovich</i>	
Fast Monte Carlo Simulation Methods Adapted to Simple Petri Net Models	370
<i>M. Estecahandy, S. Collas, L. Bordes, and C. Paroissin</i>	
Monte-Carlo Based Reliability Modelling of a Gas Network Using Graph Theory Approach	380
<i>Pavel Praks and Vytis Kopustinskas</i>	
Performance Determination for MSS Manufacturing System by Lz-Transform and Stochastic Processes Approach	387
<i>Ilia Frenkel, Svetlana Daichman, Lev Khvatskin, Neta Avraham, Oshrit Zihry, and Anatoly Lisnianski</i>	
On Availability Comparison of Reservation Modes for Multi-state Air Conditioning Systems Using Markov Approach	393
<i>Lev Khvatskin and Ilia Frenkel</i>	
Semi-Markov Modelling for Multi-state Systems	397
<i>Vlad Stefan Barbu, Alex Karagrigoriou, and Andreas Makrides</i>	
Optimizing the Availability and the Operational Cost of a Periodically Inspected Multi-state Deteriorating System with Condition Based Maintenance Policies	403
<i>S. Malefaki, V.P. Koutras, and A.N. Platis</i>	
Statistical Inference for Heavy-Tailed Distributions in Technical Systems	412
<i>Alex Karagrigoriou and Ilia Vonta</i>	
A Comparative Study of Control Charts for Zero-Inflated Binomial Processes	420
<i>Athanasios C. Rakitzis, Petros E. Maravelakis, and Philippe C. Castagliola</i>	
Practical Applications of Advanced Statistical Models in Reliability Data Analysis	426
<i>Vasily Krivtsov and Olexandr Yevkin</i>	

On Sensitivity of Reliability Models to the Shape of Life and Repair Time Distributions	430
<i>Vladimir Rykov, Dmitry Efrosinin, and Vladimir Vishnevsy</i>	

The Fourth International Workshop on Resilience and IT-Risk in Social Infrastructures (RISI 2014)

RISI I: Information and Participation for Response and Recovery

Organizing On-Site Volunteers: An App-Based Approach	438
<i>Stefan Sackmann, Marlen Hofmann, and Hans J. Betke</i>	
Visualization of Recovery Situation in Disaster Area by Using Web Reservation Data	440
<i>Yu Ichifuji and Noboru Sonehara</i>	

RISI II: k-Anonymization for Information Sharing

A k-Anonymity Method Based on Search Engine Query Statistics for Disaster Impact Statements	447
<i>Hidenobu Oguri and Noboru Sonehara</i>	
A System for Anonymizing Temporal Phrases of Message Posted in Online Social Networks and for Detecting Disclosure	455
<i>Hoang-Quoc Nguyen-Son, Minh-Triet Tran, Hiroshi Yoshiura, Sonehara Noboru, and Isao Echizen</i>	
Effects of External Information on Anonymity and Role of Transparency with Example of Social Network De-anonymisation	461
<i>Haruno Kataoka, Yohei Ogawa, Isao Echizen, Tetsuji Kuboyama, and Hiroshi Yoshiura</i>	

RISI III : Resilient Networks

Risk-Aware Design and Management of Resilient Networks	468
<i>Piotr Cholda</i>	

The First International Software Assurance Workshop (SAW 2014)

SAW I: Secure Software Architectures

Vulnerability-Based Security Pattern Categorization in Search of Missing Patterns	476
<i>Priya Anand, Jungwoo Ryoo, and Rick Kazman</i>	
Building Sustainable Software by Preemptive Architectural Design Using Tactic-Equipped Patterns	484
<i>Dae-Kyoo Kim, Jungwoo Ryoo, and Suntae Kim</i>	
Using Assurance Cases to Develop Iteratively Security Features Using Scrum	490
<i>Lotfi ben Othmane, Pelin Angin, and Bharat Bhargava</i>	

SAW II: Software Security Analysis

LiSTT: An Investigation into Unsound-Incomplete Yet Practical Result Yielding Static Taintflow Analysis	498
<i>Sanjay Rawat, Laurent Mounier, and Marie-Laure Potet</i>	

Visualization of Security Metrics for Cyber Situation Awareness	506
<i>Igor Kotenko and Evgenia Novikova</i>	

International Workshop on Security in ATM and Other Critical Infrastructures (SecATM 2014)

A Relative Cost-Benefit Approach for Evaluating Alternative Airport Security Policies	514
<i>Woohyun Shim, Fabio Massacci, Alessandra Tedeschi, and Alessandro Pollini</i>	
Mathematical Modelling in Air Traffic Management Security	523
<i>Denis Kolev and Evgeniy Morozov</i>	
The Social Acceptance of the Passivation of Misused Aircraft	530
<i>Ana P.G. Martins</i>	
EMFASE—An Empirical Framework for Security Design and Economic Trade-off	537
<i>Fabio Massacci, Federica Paci, Bjornar Solhaug, and Alessandra Tedeschi</i>	
Security Situation Management: Towards Developing a Time-Critical Decision Making Capability for SESAR	544
<i>Rainer Koelle</i>	
Design-In Security for Air Traffic Control	552
<i>Martin Hawley, Karol Gotz, John Hird, and Chris Machin</i>	
Learn to SWIM	556
<i>Matias Krempel and Martin Gilje Jaatun</i>	

The Seventh International Workshop on Digital Forensics (WSDF 2014)

Real-Time Screen Watermarking Using Overlaying Layer	561
<i>Maciej Piec and Andreas Rauber</i>	
An Efficient Intrinsic Authorship Verification Scheme Based on Ensemble Learning	571
<i>Oren Halvani and Martin Steinebach</i>	
Efficient Cropping-Resistant Robust Image Hashing	579
<i>Martin Steinebach, Huajian Liu, and York Yannikos</i>	
Author Index	586