

2013 Eighth International Conference on Availability, Reliability and Security

(ARES 2013)

**Regensburg, Germany
2-9 September**



**IEEE Catalog Number: CFP1339A-POD
ISBN: 978-1-4799-1097-7**

2013 International Conference on Availability, Reliability and Security

ARES 2013

Table of Contents

Message from the Program Committee	
Co-chairs.....	xvi
Program Committee.....	xvii
ARES 2013 Workshops: Message from the Workshop Chair.....	xxi
FARES 2013: Message from the Workshop Organizers.....	xxii
SecSE 2013: Message from the Workshop Organizers.....	xxiii
SecSE 2013: Workshop Program Committee.....	xxiv
WSDF 2013: Message from the Workshop Organizers.....	xxv
WSDF 2013: Workshop Program Committee.....	xxvi
RISI 2013: Message from the Workshop Organizers.....	xxvii
RISI 2013: Workshop Program Committee.....	xxviii
SecOnT 2013: Message from the Workshop Organizers.....	xxix
SecOnT 2013: Workshop Program Committee.....	xxx
IWSMA 2013: Message from the Workshop Organizers.....	xxxi
IWSMA 2013: Workshop Program Committee.....	xxxii
RaSIEM 2013: Message from the Workshop Organizers.....	xxxiii
RaSIEM 2013: Workshop Program Committee.....	xxxiv

ECTCM 2013: Message from the Workshop	
Organizers.....	xxxv
ECTCM 2013: Workshop Program	
Committee.....	xxxvi
RAMSS 2013: Message from the Workshop	
Organizers.....	xxxvii
RAMSS 2013: Workshop Program	
Committee.....	xxxviii
SecATM 2013: Message from the Workshop	
Organizers.....	xxxix
SecATM 2013: Workshop Program	
Committee.....	xl
ARES-IND 2013: Message from the Workshop Organizers	xli

ARES Full Papers

ARES I – Best Paper Session

Laribus: Privacy-Preserving Detection of Fake SSL Certificates with a Social P2P Notary Network	1
<i>Andrea Micheloni, Karl-Peter Fuchs, Dominik Herrmann, and Hannes Federrath</i>	
Reliability Prediction for Component-Based Software Systems with Architectural-Level Fault Tolerance Mechanisms	11
<i>Thanh-Trung Pham and Xavier Defago</i>	
A Statistical Approach for Fingerprinting Probing Activities	21
<i>Elias Bou-Harb, Mourad Debbabi, and Chadi Assi</i>	

ARES II – Risk Management & Security Models

Federated Identity Management and Usage Control - Obstacles to Industry Adoption	31
<i>Jostein Jensen and Åsmund Ahlmann Nyre</i>	
Reputation-Controlled Business Process Workflows	42
<i>Benjamin Aziz and Geoff Hamilton</i>	
Conflict Management in Obligation with Deadline Policies	52
<i>Nada Essaouini, Frédéric Cuppens, Nora Cuppens-Boulahia, and Anas Abou El Kalam</i>	

ARES III – Software Security

Validating Security Design Patterns Application Using Model Testing	62
<i>Takanori Kobashi, Nobukazu Yoshioka, Takao Okubo, Haruhiko Kaiya, Hironori Washizaki, and Yoshiaki Fukazawa</i>	
Estimating Software Vulnerabilities: A Case Study Based on the Misclassification of Bugs in MySQL Server	72
<i>Jason L. Wright, Jason W. Larsen, and Miles McQueen</i>	
Isolation of Malicious External Inputs in a Security Focused Adaptive Execution Environment	82
<i>Aaron Paulos, Partha Pal, Richard Schantz, Brett Benyo, David Johnson, Mike Hibler, and Eric Eide</i>	
PyTrigger: A System to Trigger & Extract User-Activated Malware Behavior	92
<i>Dan Fleck, Arnur Tokhtabayev, Alex Alarif, Angelos Stavrou, and Tomas Nykodym</i>	

ARES IV – Risk Planning & Threat Modeling

Run-Time Risk Management in Adaptive ICT Systems	102
<i>Mike Surridge, Bassem Nasser, Xiayou Chen, Ajay Chakravarthy, and Panos Melas</i>	
A Problem-Based Threat Analysis in Compliance with Common Criteria	111
<i>Kristian Beckers, Denis Hatebur, and Maritta Heisel</i>	
Detecting Insider Threats: A Trust-Aware Framework	121
<i>Federica Paci, Carmen Fernandez-Gago, and Francisco Moyano</i>	

ARES V – Privacy

Revisiting Circuit Clogging Attacks on Tor	131
<i>Eric Chan-Tin, Jiyoung Shin, and Jiangmin Yu</i>	
Taxonomy for Social Network Data Types from the Viewpoint of Privacy and User Control	141
<i>Christian Richthammer, Michael Netter, Moritz Riesner, and Günther Pernul</i>	
Measuring Anonymity with Plausibilistic Entropy	151
<i>I. Goriac</i>	

ARES VI – Hardware & Network Security

ARMORED: CPU-Bound Encryption for Android-Driven ARM Devices	161
<i>Johannes Götzfried and Tilo Müller</i>	
Minimizing the Costs of Side-Channel Analysis Resistance Evaluations in Early Design Steps	169
<i>Thomas Korak, Thomas Plos, and Andreas Zankl</i>	
High Availability for IPsec VPN Platforms: ClusterIP Evaluation	178
<i>Daniel Palomares, Daniel Migault, Wolfgang Velasquez, and Maryline Laurenty</i>	

ARES VII – Cryptography & Security Models

Scope of Security Properties of Sanitizable Signatures Revisited	188
<i>Hermann de Meer, Henrich C. Pöhls, Joachim Posegga, and Kai Sameli</i>	
Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme	198
<i>Jurlind Budurushi, Stephan Neumann, Maina M. Olembo, and Melanie Volkamer</i>	
The Common Limes Security Model for Asset Flow Control in Decentralized, Insecure Systems	208
<i>Eckehard Hermann and Rüdiger Grimm</i>	

ARES Short Papers

ARES VIII – Privacy & Network Security

Privacy Panel: Usable and Quantifiable Mobile Privacy	218
<i>Debmalya Biswas, Imad Aad, and Gian Paolo Perrucci</i>	
A Privacy-Preserving Entropy-Driven Framework for Tracing DoS Attacks in VoIP	224
<i>Zisis Tsiatsikas, Dimitris Geneiatakis, Georgios Kambourakis, and Angelos D. Keromytis</i>	
On Secure Multi-party Computation in Bandwidth-Limited Smart-Meter Systems	230
<i>Mario Kirschbaum, Thomas Plos, and Jörn-Marc Schmidt</i>	
Limiting MitM to MitE Covert-Channels	236
<i>Amir Herzberg and Haya Shulman</i>	

ARES IX – Threat Modeling & Intrusion Detection

Detection of Hidden Fraudulent URLs within Trusted Sites Using Lexical Features	242
<i>Enrico Sorio, Alberto Bartoli, and Eric Medvet</i>	
The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?	248
<i>Nikos Virvilis and Dimitris Gritzalis</i>	
SHPF: Enhancing HTTP(S) Session Security with Browser Fingerprinting	255
<i>Thomas Unger, Martin Mulazzani, Dominik Frühwirt, Markus Huber, Sebastian Schrittwieser, and Edgar Weippl</i>	
An Analysis and Evaluation of Security Aspects in the Business Process Model and Notation	262
<i>Maria Leitner, Michelle Miller, and Stefanie Rinderle-Ma</i>	

ARES X – Authentication, Identity Management & Trust

Resource Pool Oriented Trust Management for Cloud Infrastructure	268
<i>Gansen Zhao, Haiyu Wang, Chunming Rong, and Yong Tang</i>	
Towards Web-Based Biometric Systems Using Personal Browsing Interests	274
<i>Lukasz Olejnik and Claude Castelluccia</i>	
A Novel Proximity Based Trust Model for Opportunistic Networks	281
<i>Mai H. El-Sherief and Marianne A. Azer</i>	
The Trusted Attribute Aggregation Service (TAAS) - Providing an Attribute Aggregation Layer for Federated Identity Management	285
<i>David W. Chadwick and George Inman</i>	

ARES XI – Mobile Security

The Transitivity-of-Trust Problem in Android Application Interaction	291
<i>Steffen Bartsch, Bernhard Berger, Michaela Bunke, and Karsten Sohr</i>	
Secure Profile Provisioning Architecture for Embedded UICC	297
<i>Jaemin Park, Kiyoun Baek, and Cheoloh Kang</i>	
Ultra-lightweight Mutual Authentication Protocols: Weaknesses and Countermeasures	304
<i>Zeeshan Bilal and Keith Martin</i>	
A Reputation-Based Clustering Mechanism for MANET Routing Security	310
<i>Aida Ben Chehida, Ryma Abassi, and Sihem Guemara El Fatmi</i>	

FARES 2013

FARES I – Organizational Security Aspects (Special OSA Session)

Organizational Security Architecture for Critical Infrastructure	316
<i>Jonathan Blangenois, Guy Guemkam, Christophe Feltus, and Djamel Khadraoui</i>	
An Approach Based on Model-Driven Engineering to Define Security Policies Using OrBAC	324
<i>Denisse Muñante, Laurent Gallon, and Philippe Anioré</i>	
IT Service Continuity: Achieving Embeddedness through Planning	333
<i>Marko Niemimaa and Jonna Järveläinen</i>	

FARES II – Software Security & Testing

Enhancing Security Testing via Automated Replication of IT-Asset Topologies	341
<i>Henk Birkholz, Ingo Sieverdingbeck, Nicolai Kuntze, and Carsten Rudolph</i>	
Model-Assisted Access Control Implementation for Code-centric Ruby-on-Rails Web Application Development	350
<i>Seiji Munetoh and Nobukazu Yoshioka</i>	

A Genetic Algorithm Approach for the Most Likely Attack Path Problem	360
<i>Mohammed Alhomidi and Martin Reed</i>	
A PEP-PDP Architecture to Monitor and Enforce Security Policies in Java Applications	367
<i>Yehia Elrakaiby and Yves Le Traon</i>	

FARES III – Privacy & Forensics

iOS Forensics: How Can We Recover Deleted Image Files with Timestamp in a Forensically Sound Manner?	375
<i>Aswami Ariffin, Christian D’Orazio, Kim-Kwang Raymond Choo, and Jill Slay</i>	
Shared Crowds: A Token-Ring Approach to Hide the Receiver	383
<i>Raphael Wigoutschnigg, Peter Schartner, and Stefan Rass</i>	
On the Practicability of Cold Boot Attacks	390
<i>Michael Gruhn and Tilo Müller</i>	

FARES IV – Network & Cloud Security

DNSSEC: Interoperability Challenges and Transition Mechanisms	398
<i>Amir Herzberg and Haya Shulman</i>	
A Generation Method of Cryptographic Keys for Enterprise Communication Systems	406
<i>Aleksandar Hudic, Elise Revell, and Dimitris E. Simos</i>	
Dynamic Certification of Cloud Services	412
<i>Iryna Windhorst and Ali Sunyaev</i>	

SecSE 2013

SecSE I

Secure Engineering and Modelling of a Metering Devices System	418
<i>Jose Fran Ruiz, Marcos Arjona, Antonio Maña, and Niklas Carstens</i>	
The Use and Usefulness of Threats in Goal-Oriented Modelling	428
<i>Per Håkon Meland, Erlend Andreas Gjære, and Stéphane Paul</i>	
Modelling and Analysis of Release Order of Security Algorithms Using Stochastic Petri Nets	437
<i>Suliman A. Alsuhibany and Aad van Moorsel</i>	

SecSE II

Software Vulnerability Detection Using Backward Trace Analysis and Symbolic Execution	446
<i>Hongzhe Li, Taebeom Kim, Munkhbayar Bat-Erdene, and Heejo Lee</i>	
Automated Synthesis and Ranking of Secure BPMN Orchestrators	455
<i>V. Ciancia, F. Martinelli, I. Matteucci, M. Petrocchi, J.A. Martín, and E. Pimentel</i>	

Structured Pattern-Based Security Requirements Elicitation for Clouds	465
<i>Kristian Beckers, Maritta Heisel, Isabelle Côté, Ludger Goeke, and Selim Güler</i>	

WSDF 2013

A Comprehensive Literature Review of File Carving	475
<i>Rainer Poisel and Simon Tjoa</i>	
FASTDD: An Open Source Forensic Imaging Tool	485
<i>Paolo Bertasi and Nicola Zago</i>	
Artificial Aging of Mobile Devices Using a Simulated GSM/GPRS Network	493
<i>Rolf Stöbe, Hans Höfken, Marko Schuba, and Michael Breuer</i>	
Model-Based Generation of Synthetic Disk Images for Digital Forensic Tool Testing	498
<i>York Yannikos and Chistian Winter</i>	

RISI 2013

RISI I – Resilience and Privacy

Social Issues of Big Data and Cloud: Privacy, Confidentiality, and Public Utility	506
<i>Koichiro Hayashi</i>	
Estimating the Value of Personal Information with SNS Utility	512
<i>Memiko Otsuki and Noboru Sonehara</i>	
Anonymizing Face Images by Using Similarity-Based Metric	517
<i>Tomoya Muraki, Shintaro Oishi, Masatsugu Ichino, Isao Echizen, and Hiroshi Yoshiura</i>	

RISI II – Resilience and Safety

ICHIGAN Security - A Security Architecture That Enables Situation-Based Policy Switching	525
<i>Hiroshi Maruyama, Kiyoshi Watanabe, Sachiko Yoshihama, Naohiko Uramoto, Yoichiro Takehara, and Kazuhiro Minami</i>	
Using Twitter's Mentions for Efficient Emergency Message Propagation	530
<i>Kelly Y. Itakura and Noboru Sonehara</i>	
Towards a Risk Based Assessment of QoS Degradation for Critical Infrastructure	538
<i>Moussa Ouedraogo, Manel Khodja, and Djamel Khadraoui</i>	

SecOnT 2013

SecOnT I

A Reference Model of Information Assurance & Security	546
<i>Yulia Cherdantseva and Jeremy Hilton</i>	
An Ontology for Malware Analysis	556
<i>David A. Mundie and David M. Mcintire</i>	
A Usability Evaluation of the NESSoS Common Body of Knowledge	559
<i>Kristian Beckers and Maritta Heisel</i>	

SecOnT II

A Bootstrapping Approach for Developing a Cyber-security Ontology Using Textbook Index Terms	569
<i>Arwa Wali, Soon Ae Chun, and James Geller</i>	
Towards an Ontology for Cloud Security Obligations	577
<i>Karin Bernsmed, Astrid Undheim, Per Håkon Meland, and Martin Gilje Jaatun</i>	
On Identifying Proper Security Mechanisms	582
<i>Jakub Breier and Ladislav Hudec</i>	
Taxonomy for Port Security Systems	592
<i>Tove Gustavi and Pontus Svenson</i>	

IWMSA 2013

Probabilistic Contract Compliance for Mobile Applications	599
<i>Gianluca Dini, Fabio Martinelli, Andrea Saracino, and Daniele Sgandurra</i>	
A Classifier of Malicious Android Applications	607
<i>Gerardo Canfora, Francesco Mercaldo, and Corrado Aaron Visaggio</i>	
Privacy-Preserving Publishing of Pseudonym-Based Trajectory Location Data Set	615
<i>Ken Mano, Kazuhiro Minami, and Hiroshi Maruyama</i>	

RaSIEM 2013

RaSIEM I

A Scalable SIEM Correlation Engine and Its Application to the Olympic Games IT Infrastructure	625
<i>Valerio Vianello, Vincenzo Gulisano, Ricardo Jimenez-Peris, Marta Patiño-Martínez, Rubén Torres, Rodrigo Díaz, and Elsa Prieto</i>	
Reconsidering Intrusion Monitoring Requirements in Shared Cloud Platforms	630
<i>Kahina Lazri, Sylvie Laniepce, and Jalel Ben-Othman</i>	

RaSIEM II

The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems	638
<i>Igor Kotenko, Olga Polubelova, Igor Saenko, and Elena Doynikova</i>	
Addressing Security Issues of Electronic Health Record Systems through Enhanced SIEM Technology	646
<i>Cesario Di Sarno, Valerio Formicola, Mario Sicuranza, and Giovanni Paragliola</i>	

RaSIEM III

Experiences and Challenges in Enhancing Security Information and Event Management Capability Using Unsupervised Anomaly Detection	654
<i>Stefan Asanger and Andrew Hutchison</i>	
Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis	662
<i>Roland Rieke, Maria Zhdanova, Jürgen Repp, Romain Giot, and Chrystel Gaber</i>	

ECTCM 2013

ECTCM I

GVScan: Scanning Networks for Global Vulnerabilities	670
<i>Fabrizio Baiardi, Fabio Corò, Federico Tonelli, and Luca Guidi</i>	
Counteract DNS Attacks on SIP Proxies Using Bloom Filters	678
<i>Ge Zhang and Simone Fischer-Hübner</i>	
A Grammatical Inference Approach to Language-Based Anomaly Detection in XML	685
<i>Harald Lampesberger</i>	
Universal Peer-to-Peer Network Investigation Framework	694
<i>Mark Scanlon and M-Tahar Kechadi</i>	

ECTCM II

Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels	701
<i>Jean-Francois Lalande and Steffen Wendzel</i>	
ANANAS - A Framework for Analyzing Android Applications	711
<i>Thomas Eder, Michael Rodler, Dieter Vymazal, and Markus Zeilinger</i>	
Cuteforce Analyzer: A Distributed Bruteforce Attack on PDF Encryption with GPUs and FPGAs	720
<i>Bianca Danczul, Jürgen Fuß, Stefan Gradinger, Bernhard Greslehner, Wolfgang Kastl, and Florian Wex</i>	
Collaboratively Exchanging Warning Messages between Peers While under Attack	726
<i>Mirko Haustein, Herbert Sighart, Dennis Titze, and Peter Schoo</i>	

RAMSS 2013

Some General Properties of Multi-state Physical Models	732
<i>Paolo Rocchi and Gurami Sh. Tsitsiashvili</i>	
Assessing Water Cooling System Performance: Lz-Transform Method	737
<i>Iliia Frenkel, Lev Khvatskin, Svetlana Daichman, and Anatoly Lisnianski</i>	
Genetic Algorithm and Data Mining Techniques for Design Selection in Databases	743
<i>Christos Koukouvinos, Christina Parpoula, and Dimitris E. Simos</i>	
Statistical Inference for Multi-state Systems: The Weibull Case	747
<i>A. Makrides and A. Karagrigoriou</i>	

SecATM 2013

SecATM I

Evaluation of Airport Security Training Programs: Perspectives and Issues	753
<i>Woohyun Shim, Fabio Massacci, Martina de Gramatica, Alessandra Tedeschi, and Alessandro Pollini</i>	
ARGUS 3D: Security Enhancements through Innovative Radar Technologies	759
<i>Roberta Cardinali, Enrico Anniballi, Carlo Bongioanni, Antonio Macera, Fabiola Colone, and Pierfrancesco Lombardo</i>	

SecATM II

Enhancing CHASSIS: A Method for Combining Safety and Security	766
<i>Christian Raspotnig, Vikash Katta, Peter Karpati, and Andreas L. Opdahl</i>	
Security Blind Spots in the ATM Safety Culture	774
<i>Howard Chivers and John Hird</i>	
Requirements Management in a Combined Process for Safety and Security Assessments	780
<i>Vikash Katta, Christian Raspotnig, Peter Karpati, and Tor Stålhane</i>	
Towards Harmonising the Legislative, Regulatory, and Standards-Based Framework for ATM Security: Developing a Software Support Tool	787
<i>Rainer Koelle, Walter Strijland, and Stefan Roels</i>	

SecATM III

Sink or SWIM: Information Security Requirements in the Sky	794
<i>Martin Gilje Jaatun and Tor Erlend Fægri</i>	
Collaborative Security Management: Developing Ideas in Security Management for Air Traffic Control	802
<i>Martin Hawley, Paul Howard, Rainer Koelle, and Peter Saxton</i>	

Applying the SecRAM Methodology in a CLOUD-Based ATM Environment	807
<i>Antonio Marotta, Gabriella Carrozza, Luigi Battaglia, Patrizia Montefusco, and Vittorio Manetti</i>	
Beyond Traceability: Compared Approaches to Consistent Security Risk Assessments	814
<i>Franco Bergomi, Stéphane Paul, Bjørnar Solhaug, and Raphaël Vignon-Davillier</i>	

ARES-IND 2013

ARES-IND I

The Scourge of Internet Personal Data Collection	821
<i>Esma Aïmeur and Manuel Lafond</i>	
User Interface Harmonization for IT Security Management: User-Centered Design in the PoSecCo Project	829
<i>Beatriz Gallego-Nicasio Crespo</i>	

ARES-IND II

Overview of Recent Advances in CCTV Processing Chain in the INDECT and INSIGMA Projects	836
<i>Andrzej Dziech, Jaroslaw Bialas, Andrzej Glowacz, Pawel Korus, Mikolaj Leszczuk, Andrzej Matiolalski, and Remigiusz Baran</i>	
TRESCCA - Trustworthy Embedded Systems for Secure Cloud Computing	844
<i>Gunnar Schomaker, Andreas Herrholz, Guillaume Duc, Renaud Pacalet, Salvatore Raho, Miltos Grammatikakis, Marcello Coppola, and Ignacio Garcia Vega</i>	
Author Index	846