Message from the Program Committee

Co-chairs

Program Committee

ARES 2013 Workshops: Message from the Workshop Chair

FARES 2013: Message from the Workshop Organizers

SecSE 2013: Message from the Workshop Organizers

WSDF 2013: Message from the Workshop Organizers

RISI 2013: Message from the Workshop Organizers

SecOnT 2013: Message from the Workshop Organizers

IWSMA 2013: Message from the Workshop Organizers

RaSIEM 2013: Message from the Workshop Organizers

ARES 2013 Workshops: Message from the Workshop Chair

WSDF 2013: Workshop Program Committee

RISI 2013: Workshop Program Committee

SecOnT 2013: Workshop Program Committee

IWSMA 2013: Workshop Program Committee

RaSIEM 2013: Workshop Program Committee
ARES Full Papers

ARES I – Best Paper Session

Laribus: Privacy-Preserving Detection of Fake SSL Certificates with a Social P2P Notary Network  .................................................................1
Andrea Micheloni, Karl-Peter Fuchs, Dominik Herrmann, and Hannes Federrath

Thanh-Trung Pham and Xavier Defago

A Statistical Approach for Fingerprinting Probing Activities  .........................21
Elias Bou-Harb, Mourad Debbabi, and Chadi Assi

ARES II – Risk Management & Security Models

Federated Identity Management and Usage Control - Obstacles to Industry Adoption  .................................31
Jostein Jensen and Åsmund Ahlmann Nyre

Reputation-Controlled Business Process Workflows  ..................................42
Benjamin Aziz and Geoff Hamilton

Conflict Management in Obligation with Deadline Policies  .............................52
Nada Essaouini, Frédéric Cuppens, Nora Cuppens-Boulahia, and Anas Abou El Kalam
ARES III – Software Security
Validating Security Design Patterns Application Using Model Testing ..........................................................62
  Takanori Kobashi, Nobukazu Yoshioka, Takao Okubo, Haruhiko Kaiya,
  Hironori Washizaki, and Yoshiaki Fukazawa
Estimating Software Vulnerabilities: A Case Study Based on the Misclassification of Bugs in MySQL Server .................................................................72
  Jason L. Wright, Jason W. Larsen, and Miles McQueen
Isolation of Malicious External Inputs in a Security Focused Adaptive Execution Environment ...........................................................................................................................................................................................................................................82
  Aaron Paulos, Partha Pal, Richard Schantz, Brett Benyo, David Johnson,
  Mike Hibler, and Eric Eide
PyTrigger: A System to Trigger & Extract User-Activated Malware Behavior .........................................................92
  Dan Fleck, Arnur Tokhtabayev, Alex Alarif, Angelos Stavrou,
  and Tomas Nykodym

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

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

ARES VI – Hardware & Network Security
ARMORED: CPU-Bound Encryption for Android-Driven ARM Devices .................................................................161
  Johannes Götzfried and Tilo Müller
Minimizing the Costs of Side-Channel Analysis Resistance Evaluations in Early Design Steps ..................................169
  Thomas Korak, Thomas Plos, and Andreas Zankl
High Availability for IPsec VPN Platforms: ClusterIP Evaluation ..............................................................................178
  Daniel Palomares, Daniel Migault, Wolfgang Velasquez, and Maryline Laurenty
ARES VII – Cryptography & Security Models

Scope of Security Properties of Sanitizable Signatures Revisited .....................................................188
Hermann de Meer, Henrich C. Pöhls, Joachim Posegga, and Kai Sameli

Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme .................................................................198
Jurilind Budurushi, Stephan Neumann, Maina M. Olembo, and Melanie Volkamer

The Common Limes Security Model for Asset Flow Control in Decentralized, Insecure Systems ...............................................................208
Eckehard Hermann and Rüdiger Grimm

ARES Short Papers

ARES VIII – Privacy & Network Security

Privacy Panel: Usable and Quantifiable Mobile Privacy .................................................................218
Debmalya Biswas, Imad Aad, and Gian Paolo Perrucci

A Privacy-Preserving Entropy-Driven Framework for Tracing DoS Attacks in VoIP ..........................................................224
Zisis Tsiatsikas, Dimitris Geneiatakis, Georgios Kambourakis, and Angelos D. Keromytis

On Secure Multi-party Computation in Bandwidth-Limited Smart-Meter Systems .................................................................230
Mario Kirschbaum, Thomas Plos, and Jörn-Marc Schmidt

Limiting MitM to MitE Covert-Channels ..................................................................................236
Amir Herzberg and Haya Shulman

ARES IX – Threat Modeling & Intrusion Detection

Detection of Hidden Fraudulent URLs within Trusted Sites Using Lexical Features ...........................................................................242
Enrico Sorio, Alberto Bartoli, and Eric Medvet

The Big Four - What We Did Wrong in Advanced Persistent Threat Detection? ..................................................................................248
Nikos Virvilis and Dimitris Gritzalis

SHPF: Enhancing HTTP(S) Session Security with Browser Fingerprinting ..................................................255
Thomas Unger, Martin Mulazzani, Dominik Frühwirt, Markus Huber, Sebastian Schrittwieser, and Edgar Weippl

An Analysis and Evaluation of Security Aspects in the Business Process Model and Notation ...................................................................262
Maria Leitner, Michelle Miller, and Stefanie Rinderle-Ma
ARES X – Authentication, Identity Management & Trust
Resource Pool Oriented Trust Management for Cloud Infrastructure ...........................................268
Gansen Zhao, Haiyu Wang, Chunming Rong, and Yong Tang
Towards Web-Based Biometric Systems Using Personal Browsing Interests ........................................274
Lukasz Olejnik and Claude Castelluccia
A Novel Proximity Based Trust Model for Opportunistic Networks .........................................................281
Mai H. El-Sherief and Marianne A. Azer
The Trusted Attribute Aggregation Service (TAAS) - Providing an Attribute Aggregation Layer for Federated Identity Management ..........................................................................................................................285
David W. Chadwick and George Inman

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

FARES 2013

FARES I – Organizational Security Aspects (Special OSA Session)
Organizational Security Architecture for Critical Infrastructure .................................................................316
Jonathan Blangenois, Guy Guemkam, Christophe Feltus, and Djamel Khadraoui
An Approach Based on Model-Driven Engineering to Define Security Policies Using OrBAC ..........................................................324
Denisse Muñante, Laurent Gallon, and Philippe Aniortè
IT Service Continuity: Achieving Embeddedness through Planning ...................................................333
Marko Niemimaa and Jonna Järveläinen

FARES II – Software Security & Testing
Enhancing Security Testing via Automated Replication of IT-Asset Topologies ..................................................341
Henk Birkholz, Ingo Sieverdingbeck, Nicolai Kuntze, and Carsten Rudolph
Model-Assisted Access Control Implementation for Code-centric Ruby-on-Rails Web Application Development ..........................................................350
Seiji Munetoh and Nobukazu Yoshioka
A Genetic Algorithm Approach for the Most Likely Attack Path Problem ..................................................360
Mohammed Alhomidi and Martin Reed

A PEP-PDP Architecture to Monitor and Enforce Security Policies in Java Applications ........................................................................................................................................367
Yehia Elrakaiby and Yves Le Traon

**FARES III – Privacy & Forensics**

iOS Forensics: How Can We Recover Deleted Image Files with Timestamp in a Forensically Sound Manner? ........................................................................................................................................375
Aswami Ariffin, Christian D'Oorazio, Kim-Kwang Raymond Choo, and Jill Slay

Shared Crowds: A Token-Ring Approach to Hide the Receiver ...........................................................................383
Raphael Wigoutschnigg, Peter Schartner, and Stefan Rass

On the Practicability of Cold Boot Attacks .......................................................................................................390
Michael Gruhn and Tilo Müller

**FARES IV – Network & Cloud Security**

DNSSEC: Interoperability Challenges and Transition Mechanisms ..........................................................398
Amir Herzberg and Haya Shulman

Aleksandar Hudic, Elise Revell, and Dimitris E. Simos

Dynamic Certification of Cloud Services ...........................................................................................................412
Iryna Windhorst and Ali Sunyaev

**SecSE 2013**

**SecSE I**

Secure Engineering and Modelling of a Metering Devices System .................................................................418
Jose Fran Ruiz, Marcos Arjona, Antonio Maña, and Niklas Carstens

The Use and Usefulness of Threats in Goal-Oriented Modelling .......................................................................428
Per Håkon Meland, Erlend Andreas Gjære, and Stéphane Paul

Modelling and Analysis of Release Order of Security Algorithms Using Stochastic Petri Nets ..................437
Suliman A. Alsuhibany and Aad van Moorsel

**SecSE II**

Software Vulnerability Detection Using Backward Trace Analysis and Symbolic Execution ................................446
Hongzhe Li, Taebeom Kim, Munkhbayar Bat-Erdene, and Heejo Lee

Automated Synthesis and Ranking of Secure BPMN Orchestrators .................................................................455
V. Ciancia, F. Martinelli, I. Matteucci, M. Petrocchi, J.A. Martin, and E. Pimentel
Structured Pattern-Based Security Requirements Elicitation for Clouds .................................................................465
    Kristian Beckers, Maritta Heisel, Isabelle Côté, Ludger Goeke, and Selim Güler

**WSDF 2013**

A Comprehensive Literature Review of File Carving .................................................................................475
    Rainer Poisel and Simon Tjoa

FASTDD: An Open Source Forensic Imaging Tool ......................................................................................485
    Paolo Bertasi and Nicola Zago

Artificial Aging of Mobile Devices Using a Simulated GSM/GPRS Network .................................................493
    Rolf Stöbe, Hans Höfken, Marko Schuba, and Michael Breuer

Model-Based Generation of Synthetic Disk Images for Digital Forensic Tool Testing ..................................498
    York Yannikos and Christian Winter

**RISI 2013**

**RISI I – Resilience and Privacy**

Social Issues of Big Data and Cloud: Privacy, Confidentiality, and Public Utility ...........................................506
    Koichiro Hayashi

Estimating the Value of Personal Information with SNS Utility .................................................................512
    Memiko Otsuki and Noboru Sonehara

Anonymizing Face Images by Using Similarity-Based Metric .................................................................517
    Tomoya Muraki, Shintaro Oishi, Masatsugu Ichino, Isao Echizen, and Hiroshi Yoshiura

**RISI II – Resilience and Safety**

ICHIGAN Security - A Security Architecture That Enables Situation-Based Policy Switching ....................525
    Hiroshi Maruyama, Kiyoshi Watanabe, Sachiko Yoshihama, Naohiko Uramoto, Yoichiro Takehora, and Kazuhiro Minami

Using Twitter's Mentions for Efficient Emergency Message Propagation .................................................530
    Kelly Y. Itakura and Noboru Sonehara

Towards a Risk Based Assessment of QoS Degradation for Critical Infrastructure ....................................538
    Moussa Ouedraogo, Manel Khodja, and Djamel Khadraoui

**SecOnT 2013**
SecOnT I
A Reference Model of Information Assurance & Security ..................................................546
  Yulia Cherdantseva and Jeremy Hilton
An Ontology for Malware Analysis ..............................................................................556
  David A. Mundie and David M. McIntire
A Usability Evaluation of the NESSoS Common Body of Knowledge ......................559
  Kristian Beckers and Maritta Heisel

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

IWMSA 2013
Probabilistic Contract Compliance for Mobile Applications ......................................599
  Gianluca Dini, Fabio Martinelli, Andrea Saracino, and Daniele Sgandurra
A Classifier of Malicious Android Applications ............................................................607
  Gerardo Canfora, Francesco Mercaldo, and Corrado Aaron Visaggio
Privacy-Preserving Publishing of Pseudonym-Based Trajectory Location
Data Set ..........................................................................................................................615
  Ken Mano, Kazuhiro Minami, and Hiroshi Maruyama

RaSIEM 2013

RaSIEM I
A Scalable SIEM Correlation Engine and Its Application to the Olympic Games IT Infrastructure .............................................................625
  Valerio Vianello, Vincenzo Gulisano, Ricardo Jimenez-Peris,
  Marta Patiño-Martínez, Rubén Torres, Rodrigo Díaz, and Elsa Prieto
Reconsidering Intrusion Monitoring Requirements in Shared Cloud Platforms .............630
  Kahina Lazri, Sylvie Lanierpce, and Jalel Ben-Othman
RaSIEM II
The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems
Igor Kotenko, Olga Polubelova, Igor Saenko, and Elena Doynikova

Addressing Security Issues of Electronic Health Record Systems through Enhanced SIEM Technology
Cesario Di Sarno, Valerio Formicola, Mario Sicuranza, and Giovanni Paragliola

RaSIEM III
Experiences and Challenges in Enhancing Security Information and Event Management Capability Using Unsupervised Anomaly Detection
Stefan Asanger and Andrew Hutchison

Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis
Roland Rieke, Maria Zhdanova, Jürgen Repp, Romain Giot, and Chrystel Gaber

ECTCM 2013

ECTCM I
GVScan: Scanning Networks for Global Vulnerabilities
Fabrizio Baiardi, Fabio Corò, Federico Tonelli, and Luca Guidi

Counteract DNS Attacks on SIP Proxies Using Bloom Filters
Ge Zhang and Simone Fischer-Hübner

A Grammatical Inference Approach to Language-Based Anomaly Detection in XML
Harald Lampesberger

Universal Peer-to-Peer Network Investigation Framework
Mark Scanlon and M-Tahar Kechadi

ECTCM II
Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels
Jean-Francois Lalande and Steffen Wendzel

ANANAS - A Framework for Analyzing Android Applications
Thomas Eder, Michael Rodler, Dieter Vymazal, and Markus Zeilinger

Cuteforce Analyzer: A Distributed Bruteforce Attack on PDF Encryption with GPUs and FPGAs
Bianca Danczul, Jürgen Fuß, Stefan Gradinger, Bernhard Greslehner, Wolfgang Kastl, and Florian Wex

Collaboratively Exchanging Warning Messages between Peers While under Attack
Mirko Haustein, Herbert Sighart, Dennis Titze, and Peter Schoo
RAMSS 2013

Some General Properties of Multi-state Physical Models ..........................................................732
  Paolo Rocchi and Gurami Sh. Tsitsiashvili

Assessing Water Cooling System Performance: Lz-Transform Method ......................................737
  Ilia Frenkel, Lev Khvatkskin, Svetlana Daichman, and Anatoly Lisnianski

Genetic Algorithm and Data Mining Techniques for Design Selection in Databases .........................743
  Christos Koukouvinos, Christina Parpoula, and Dimitris E. Simos

Statistical Inference for Multi-state Systems: The Weibull Case ..................................................747
  A. Makrides and A. Karagrigoriou

SecATM 2013

SecATM I

Evaluation of Airport Security Training Programs: Perspectives and Issues ....................................753
  Woohyun Shim, Fabio Massacci, Martina de Gramatica, Alessandra Tedeschi, and Alessandro Pollini

ARGUS 3D: Security Enhancements through Innovative Radar Technologies ....................................759
  Roberta Cardinali, Enrico Anniballi, Carlo Bongioanni, Antonio Macera, Fabiola Colone, and Pierfrancesco Lombardo

SecATM II

Enhancing CHASSIS: A Method for Combining Safety and Security ..............................................766
  Christian Raspotnig, Vikash Katta, Peter Karpati, and Andreas L. Opdahl

Security Blind Spots in the ATM Safety Culture ............................................................................774
  Howard Chivers and John Hird

Requirements Management in a Combined Process for Safety and Security Assessments ..................780
  Vikash Katta, Christian Raspotnig, Peter Karpati, and Tor Stålhane

Towards Harmonising the Legislative, Regulatory, and Standards-Based Framework for ATM Security: Developing a Software Support Tool .........................................................787
  Rainer Koelle, Walter Strijland, and Stefan Roels

SecATM III

Sink or SWIM: Information Security Requirements in the Sky .....................................................794
  Martin Gilje Jaatun and Tor Erlend Fægri

Collaborative Security Management: Developing Ideas in Security Management for Air Traffic Control ..............................................................802
  Martin Hawley, Paul Howard, Rainer Koelle, and Peter Saxton
Applying the SecRAM Methodology in a CLOUD-Based ATM Environment .................................................807
  Antonio Marotta, Gabriella Carrozza, Luigi Battaglia, Patrizia Montefusco,
  and Vittorio Manetti

Beyond Traceability: Compared Approaches to Consistent Security Risk Assessments .................................................................814
  Franco Bergomi, Stéphane Paul, Bjørnar Solhaug, and Raphaël Vignon-Davillier

ARES-IND 2013

ARES-IND I

The Scourge of Internet Personal Data Collection .........................................................................................821
  Esma Aïmeur and Manuel Lafond

User Interface Harmonization for IT Security Management: User-Centered Design in the PoSecCo Project ........................................................829
  Beatriz Gallego-Nicasio Crespo

ARES-IND II

Overview of Recent Advances in CCTV Processing Chain in the INDECT and INSIGMA Projects ........................................................................836
  Andrzej Dziech, Jaroslaw Bialas, Andrzej Glowacz, Pawel Korus,
  Mikolaj Leszczuk, Andrzej Matiolalski, and Remigiusz Baran

TRESCCA - Trustworthy Embedded Systems for Secure Cloud Computing ...............................................844
  Gunnar Schomaker, Andreas Herrholz, Guillaume Duc, Renaud Pacalet,
  Salvatore Raho, Miltos Grammatikakis, Marcello Coppola,
  and Ignacio Garcia Vega

Author Index ..................................................................................................................................................846