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

Reliability Prediction for Component-Based Software Systems with Architectural-Level Fault Tolerance Mechanisms .............................................................................11
   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, Amur 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 Hategur, 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
   Jurlind 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 Schrittewieser, 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

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

## ARES XI – Mobile Security

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

## FARES 2013

### FARES I – Organizational Security Aspects (Special OSA Session)

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

### FARES II – Software Security & Testing

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

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 Laniepce, and Jalel Ben-Othman
RaSIEM II
The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems .................................................................................................................638
Igor Kotenko, Olga Polubelova, Igor Saenko, and Elena Doynikova

Addressing Security Issues of Electronic Health Record Systems through Enhanced SIEM Technology ...........................................................................646
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 ........................................654
Stefan Asanger and Andrew Hutchison

Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis ..................................................................................................................662
Roland Rieke, Maria Zhdanova, Jürgen Repp, Romain Giot, and Chrystel Gaber

ECTCM 2013
ECTCM I
GVScan: Scanning Networks for Global Vulnerabilities ........................................670
Fabrizio Baiardi, Fabio Corò, Federico Tonelli, and Luca Guidi

Counteract DNS Attacks on SIP Proxies Using Bloom Filters ..................................678
Ge Zhang and Simone Fischer-Hübner

A Grammatical Inference Approach to Language-Based Anomaly Detection in XML .............................................................................................................685
Harald Lampesberger

Universal Peer-to-Peer Network Investigation Framework ........................................694
Mark Scanlon and M-Tahar Kechadi

ECTCM II
Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels ...............................................................................................................701
Jean-Francois Lalande and Steffen Wendzel

ANANAS - A Framework for Analyzing Android Applications ..................................711
Thomas Eder, Michael Rodler, Dieter Vymazal, and Markus Zeilinger

Cuteforce Analyzer: A Distributed Bruteforce Attack on PDF Encryption with GPUs and FPGAs .........................................................................................720
Bianca Danczul, Jürgen Fuß, Stefan Gradinger, Bernhard Greslehner, Wolfgang Kastl, and Florian Wex

Collaboratively Exchanging Warning Messages between Peers While under Attack ............................................................................................................726
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 Khvatskin, 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

xiv
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, Jarosław Białas, Andrzej Glowacz, Paweł Korus, Mikołaj Leszczuk, Andrzej Matiolski, 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 García Vega

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