

2016 11th International Conference on Availability, Reliability and Security (ARES 2016)

**Salzburg, Austria
31 August – 2 September 2016**



**IEEE Catalog Number: CFP1639A-POD
ISBN: 978-1-5090-0991-6**

**Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1639A-POD
ISBN (Print-On-Demand):	978-1-5090-0991-6
ISBN (Online):	978-1-5090-0990-9

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2016 11th International Conference on Availability, Reliability and Security

ARES 2016

Table of Contents

Message from the ARES 2016 Program Committee Co-Chairs.....	xviii
ARES 2016 Organizing Committee.....	xix
ARES 2016 Program Committee.....	xx
Message from the ARES 2016 Workshop Chair.....	xxii
Message from the FARES 2016 Workshop Organizers.....	xxiii
Message from the WSDF 2016 Workshop Organizers.....	xxiv
WSDF 2016 Program Committee.....	xxv
Message from the IWSMA 2016 Workshop Organizers.....	xxvi
IWSMA 2016 Program Committee.....	xxvii
Message from the IWCC 2016 Workshop Organizers.....	xxviii
IWCC 2016 Program Committee.....	xxix
Message from the SAW 2016 Workshop Organizers.....	xxx
SAW 2016 Program Committee.....	xxxI
Message from the SecATM 2016 Workshop Organizers.....	xxxii
SecATM 2016 Program Committee.....	xxxiii
Message from the ASSD 2016 Workshop Organizers.....	xxxiv
ASSD 2016 Program Committee.....	xxxv
Message from the WMA 2016 Workshop Organizers.....	xxxvi

WMA 2016 Program Committee	xxxvii
Message from the ISPM 2016 Workshop	
Organizers	xxxviii
ISPM 2016 Program Committee	xxxix
Message from the ARES 2016 EU Projects	
Symposium	xl
Message from the FASES 2016 Workshop	
Organizers	xli
FASES 2016 Program Committee	xlii
Message from the SECPID 2016 Workshop	
Organizers	xliii
SECPID 2016 Program Committee	xliv
Message from the MUIIN 2016 Workshop	
Organizers	xliv
MUIIN 2016 Program Committee	xlvi
Message from the SOCOTUD 2016	
Workshop Organizers	xlvii
SOCOTUD 2016 Program Committee	xlviii

ARES Full Papers

ARES Full I: Best Paper Session

A Recommender-Based System for Assisting Non-technical Users in Managing Android Permissions	1
<i>Arnaud Oglaza, Romain Laborde, Abdelmalek Benzekri, and François Barrère</i>	
No Need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large	10
<i>Wilfried Mayer, Aaron Zauner, Martin Schmiedecker, and Markus Huber</i>	
Revisiting a Watermark-Based Detection Scheme to Handle Cyber-Physical Attacks	21
<i>José Rubio-Hernán, Luca De Cicco, and Joaquín García-Alfaro</i>	

ARES Full II: Cryptography

Byzantine Set-Union Consensus Using Efficient Set Reconciliation	29
<i>Florian Dold and Christian Grothoff</i>	
k-Times Full Traceable Ring Signature	39
<i>Xavier Bultel and Pascal Lafourcade</i>	

Towards Cycle-Accurate Emulation of Cortex-M Code to Detect Timing Side Channels	49
<i>Johannes Bauer and Felix Freiling</i>	

ARES Full III: Network and Software Security

POTR: Practical On-the-Fly Rejection of Injected and Replayed 802.15.4 Frames	59
<i>Konrad-Felix Krentz, Christoph Meinel, and Maxim Schnjakin</i>	
Stopping Amplified DNS DDoS Attacks through Distributed Query Rate Sharing	69
<i>Saurabh Verma, Ali Hamieh, Jun Ho Huh, Henrik Holm, Siva Raj Rajagopalan, Maciej Korczynski, and Nina Fefferman</i>	
HyperCrypt: Hypervisor-Based Encryption of Kernel and User Space	79
<i>Johannes Götzfried, Nico Dörr, Ralph Palutke, and Tilo Müller</i>	

ARES Full IV: Privacy-Enhancing Technologies

Efficient and Privacy Preserving Third Party Auditing for a Distributed Storage System	88
<i>Denise Demirel, Stephan Krenn, Thomas Lorünser, and Giulia Traverso</i>	
Introducing Proxy Voting to Helios	98
<i>Oksana Kulyk, Karola Marky, Stephan Neumann, and Melanie Volkamer</i>	

ARES Full V: Applications

ARTIST: The Android Runtime Instrumentation Toolkit	107
<i>Lukas Dresel, Mykolai Protsenko, and Tilo Müller</i>	
Development of an AUTOSAR Compliant Cryptographic Library on State-of-the-Art Automotive Grade Controllers	117
<i>Pal-Stefan Murvay, Alexandru Matei, Cristina Solomon, and Bogdan Groza</i>	
Using Expert Systems to Statically Detect "Dynamic" Conflicts in XACML	127
<i>Bernard Stepien and Amy Felty</i>	

ARES Full VI: Intrusion Detection and Incident Response

Selection of Mitigation Actions Based on Financial and Operational Impact Assessments	137
<i>Gustavo Gonzalez Granadillo, Alexander Motzek, Joaquin Garcia-Alfaro, and Hervé Debar</i>	
A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow	147
<i>Mehdi Nobakht, Vijay Sivaraman, and Roksana Boreli</i>	
Towards a CDS-based Intrusion Detection Deployment Scheme for Securing Industrial Wireless Sensor Networks	157
<i>Lyes Bayou, Nora Cuppens-Boulahia, David Espès, and Frédéric Cuppen</i>	

ARES Full VII: Security Models and Architectures

Role Mining with Missing Values	167
<i>Sokratis Vavilis, Alexandru Ionut Egner, Milan Petković, and Nicola Zannone</i>	
Towards a Systemic Approach for Information Security Risk Management	177
<i>Yannick Naudet, Nicolas Mayer, and Christophe Feltus</i>	
Towards a Metamodel for SABSA Conceptual Architecture Descriptions	187
<i>Patrick Pleinevaux</i>	
Threat Modelling Service Security as a Security Ceremony	195
<i>Taciane Martimiano and Jean Everson Martina</i>	

ARES Short Papers

ARES Short I: Cloud Security

Access Control and Data Separation Metrics in Cloud Infrastructures	205
<i>Bernd Jaeger, Reiner Kraft, Sebastian Luhn, Annika Selzer, and Ulrich Waldmann</i>	
IFCaaS: Information Flow Control as a Service for Cloud Security	211
<i>Marwa Elsayed and Mohammad Zulkernine</i>	
Your Cloud in My Company: Modern Rights Management Services Revisited	217
<i>Martin Grothe, Christian Mainka, Paul Rösler, Johanna Jupke, Jan Kaiser, and Jörg Schwenk</i>	

ARES Short II: Applications

A Hazus-Based Method for Assessing Robustness of Electricity Supply to Critical Smart Grid Consumers during Flood Events	223
<i>Alexandr Vasenev, Lorena Montoya, and Andrea Ceccarelli</i>	
Hybrid Focused Crawling for Homemade Explosives Discovery on Surface and Dark Web	229
<i>Christos Iliou, George Kalpakis, Theodora Tsikrika, Stefanos Vrochidis, and Ioannis Kompatsiaris</i>	
The Case for RAID 4: Cloud-RAID Integration with Local Storage	235
<i>Christopher Hansen and James Archibald</i>	
An Empirical Study on GSN Usage Intention: Factors Influencing the Adoption of Geo-Social Networks	241
<i>Esma Aïmeur, Sébastien Gambs, and Cheu Yien Yep</i>	

ARES Short III: Cryptography

Energy Efficient Mutual Authentication and Key Agreement Scheme with Strong Anonymity Support for Secure Ubiquitous Roaming Services	247
<i>Prosanta Gope, Ruei-Hau Hsu, Jemin Lee, and Tony Q. S. Quek</i>	
Provable User Authentication Scheme in Telecare Medicine Information System Using Elliptic Curve Cryptosystem	253
<i>Toan Thinh Truong, Duong Tien Phan, Minh Triet Tran, Anh Duc Duong, and Isao Echizen</i>	
Synchronous One Time Biometrics with Pattern Based Authentication	260
<i>Patrick Lacharme and Christophe Rosenberger</i>	
V-DIFT: Vector-Based Dynamic Information Flow Tracking with Application to Locating Cryptographic Keys for Reverse Engineering	266
<i>Antonio M. Espinoza, Jeffrey Knockel, Pedro Comesaña-Alfaro, and Jedidiah R. Crandall</i>	

ARES Short IV: Security Methods

Usable Privacy-Aware Logging for Unstructured Log Entries	272
<i>Christof Rath</i>	
pwnPr3d: An Attack-Graph-Driven Probabilistic Threat-Modeling Approach	278
<i>Pontus Johnson, Alexandre Verotte, Mathias Ekstedt, and Robert Lagerström</i>	
The Landscape of Domain Name Typosquatting: Techniques and Countermeasures	284
<i>Jeffrey Spaulding, Shambhu Upadhyaya, and Aziz Mohaisen</i>	

FARES 2016

FARES I: International Workshop on Frontiers in Availability, Reliability and Security

Caller-Centrality: Identifying Telemarketers in a VoIP Network	290
<i>Muhammad Ajmal Azad and Syed Khurram Rizvi</i>	
Collaborative Attribute Retrieval in Environment with Faulty Attribute Managers	296
<i>Mario Faiella, Fabio Martinelli, Paolo Mori, Andrea Saracino, and Mina Sheikhalishahi</i>	
Recognizing Time-Efficiently Local Botnet Infections - A Case Study	304
<i>Tanja Heuer, Ina Schiering, Frank Klawnn, Alexander Gabel, and Martin Seeger</i>	
VoIP Profiler: Profiling Voice over IP User Communication Behavior	312
<i>Sainath Batthalla, Mayank Swarnkar, Neminath Hubballi, and Maitreya Natu</i>	

WSDF 2016

WSDF I: Mobile and OS Forensics

Identification and Analysis of Email and Contacts Artefacts on iOS and OS X	321
<i>Kenneth M. Ovens and Gordon Morison</i>	
Extraction and Analysis of Volatile Memory in Android Systems: An Approach Focused on Trajectory Reconstruction Based on NMEA 0183 Standard	328
<i>João Paulo Claudino de Sousa and João José Costa Gondim</i>	
Digital Forensic Artifacts of the Cortana Device Search Cache on Windows 10 Desktop	338
<i>Patricio Domingues and Miguel Frade</i>	

WSDF II: Cloud Forensics

A Forensic Acquisition and Analysis System for IaaS: Architectural Model and Experiment	345
<i>Saad Alqahtany, Nathan Clarke, Steven Furnell, and Christoph Reich</i>	
A Log-Structured Block Preservation and Restoration System for Proactive Forensic Data Collection in the Cloud	355
<i>Manabu Hirano and Hiromu Ogawa</i>	

IWSMA 2016

IWSMA I: International Workshop on Security of Mobile Applications

Notary-Assisted Certificate Pinning for Improved Security of Android Apps	365
<i>Georg Merzdovnik, Damjan Buhov, Artemios G. Voyiatzis, and Edgar R. Weippl</i>	
Spotting the Malicious Moment: Characterizing Malware Behavior Using Dynamic Features	372
<i>Alberto Ferrante, Eric Medvet, Francesco Mercaldo, Jelena Milosevic, and Corrado Aaron Visaggio</i>	

IWSMA II: International Workshop on Security of Mobile Applications

Lightweight Encryption for Smart Home	382
<i>Sanaah Al Salami, Joonsang Baek, Khaled Salah, and Ernesto Damiani</i>	
Hand Dynamics for Behavioral User Authentication	389
<i>Fuensanta Torres Garcia, Katharina Krombholz, Rudolf Mayer, and Edgar Weippl</i>	

IWCC 2016

IWCC I: International Workshop on Cyber Crime

Law Enforcement Access to Password Protected and/or Encrypted Mobile Data	399
<i>Murdoch Watney</i>	
Towards Digital Investigation in Virtual Networks: A Study of Challenges and Open Problems	406
<i>Daniel Spiekermann and Tobias Eggendorfer</i>	
Threat from Within: Case Studies of Insiders Who Committed Information Technology Sabotage	414
<i>Jason W. Clark</i>	
Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers	423
<i>S. Kumar, L. Madhavan, M. Nagappan, and B. Sikdar</i>	

SAW 2016

SAW I: International Software Assurance Workshop

Towards a Unified Secure Cloud Service Development and Deployment Life-Cycle	428
<i>Aleksandar Hudic, Matthias Flittner, Thomas Lorünser, Philipp M. Radl, and Roland Bless</i>	
A Security Game Model for Remote Software Protection	437
<i>Nicola Basilico, Andrea Lanzi, and Mattia Monga</i>	
SPARER: Secure Cloud-Proof Storage for e-Health Scenarios	444
<i>Gabriela Gheorghe, Muhammad Rizwan Asghar, Jean Lancrenon, and Sankalp Ghatpande</i>	

SAW II: International Software Assurance Workshop

How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection	454
<i>Nikhil Tripathi, Neminath Hubballi, and Yogendra Singh</i>	
A Type System for Quantified Information-Flow Security in Java-Like Languages	464
<i>Gohar Shakoori, Mehran S. Fallah, and Zeinab Iranmanesh</i>	
On Analyzing Program Behavior under Fault Injection Attacks	474
<i>Jakub Breier</i>	

SAW III: International Software Assurance Workshop

Authentication in the Context of E-Participation: Current Practice, Challenges and Recommendations	480
<i>Maria Leitner and Arndt Bonitz</i>	

SecATM 2016

SecATM I: ATM Security Research and Development

Air Traffic Management Security Research in SESAR	486
<i>John Hird, Martin Hawley, and Chris Machin</i>	
A New Vision for ATM Security Management: The Security Management Platform	493
<i>Claudio Porretti, Raoul Lahaije, and Denis Kolev</i>	
'CTRL_S' - A Security Tool for SESAR's Design-In Security Approach	499
<i>Karol Gotz, Martin Hawley, Chris Machin, and John Hird</i>	

SecATM II: Risk Assessment and Incident Management

Security Risk Assessment and Risk Treatment for Integrated Modular Communication	503
<i>Hamid Asgari, Sarah Haines, and Adrian Waller</i>	
Cyber Security Incident Management in the Aviation Domain	510
<i>Martin Gilje Jaatun and Rainer Koelle</i>	
A Model-Based Approach for Aviation Cyber Security Risk Assessment	517
<i>Tobias Kiesling, Matias Krempel, Josef Niederl, and Jürgen Ziegler</i>	

SecATM III: Testing and Validation

Security Testing with Controller-Pilot Data Link Communications	526
<i>Doris Di Marco, Alessandro Manzo, Marco Ivaldi, and John Hird</i>	
Addressing Security in the ATM Environment: From Identification to Validation of Security Countermeasures with Introduction of New Security Capabilities in the ATM System Context	532
<i>Patrizia Montefusco, Rosana Casar, Rainer Koelle, and Tim H. Stelkens-Kobsch</i>	

ASSD 2016

ASSD I: Secure DevOps

SecDevOps: Is It a Marketing Buzzword? - Mapping Research on Security in DevOps	542
<i>Vaishnavi Mohan and Lotfi Ben Othmane</i>	

ASSD II: Experiences in Agile Development of Secure Software

An Empirical Study on the Relationship between Software Security Skills, Usage and Training Needs in Agile Settings	548
<i>Tosin Daniel Oyetoyan, Daniela Soares Cruzes, and Martin Gilje Jaatun</i>	
Case Study of Security Development in an Agile Environment: Building Identity Management for a Government Agency	556
<i>Kalle Rindell, Sami Hyrynsalmi, and Ville Leppänen</i>	
Towards Effective Security Assurance for Incremental Software Development the Case of Zen Cart Application	564
<i>Lotfi Ben Othmane and Azmat Ali</i>	

ASSD III: Assessment of Research on Agile Development of Secure Software

Misuse, Abuse and Reuse: Economic Utility Functions for Characterising Security Requirements	572
<i>Chad Heitzenrater and Andrew Simpson</i>	
Agile Team Members Perceptions on Non-functional Testing: Influencing Factors from an Empirical Study	582
<i>Cristina Rosa Camacho, Sabrina Marczak, and Daniela S. Cruzes</i>	

WMA 2016

WMA I: International Workshop on Malware Analysis

A Peek under the Hood of iOS Malware	590
<i>Laura García and Ricardo J. Rodríguez</i>	

WMA II: International Workshop on Malware Analysis

What's Your Major Threat? On the Differences between the Network Behavior of Targeted and Commodity Malware	599
<i>Enrico Mariconti, Jeremiah Onalapo, Gordon Ross, and Gianluca Stringhini</i>	
Exploring the Usage of Topic Modeling for Android Malware Static Analysis	609
<i>Eric Medvet and Francesco Meraldo</i>	
Classification of Short Messages Initiated by Mobile Malware	618
<i>Marian Kühnel and Ulrike Meyer</i>	

WMA III: International Workshop on Malware Analysis

Ransomware Inside Out	628
<i>Francesco Meraldo, Vittoria Nardone, and Antonella Santone</i>	

Detecting Packed Executable File: Supervised or Anomaly Detection Method?	638
<i>Neminath Hubballi and Himanshu Dogra</i>	

ISPM 2016

ISPM I: Challenges, Threats and Solutions

The Perfect Storm: The Privacy Paradox and the Internet-of-Things	644
<i>Meredydd Williams, Jason R. C. Nurse, and Sadie Creese</i>	

ISPM II: Models and Communication

Privacy Impact Assessment Template for Provenance	653
<i>Jenni Reuben, Leonardo A. Martucci, Simone Fischer-Hübner, Heather S. Packer, Hans Hedbom, and Luc Moreau</i>	

Major Challenges in Structuring and Institutionalizing CERT-Communication	661
<i>Otto Hellwig, Gerald Quirchmayr, Edith Huber, Gernot Goluch, Franz Vock, and Bettina Pospisil</i>	

Towards a Complex Systems Approach to Legal and Economic Impact Analysis of Critical Infrastructures	668
<i>Thomas Schaberreiter, Gerald Quirchmayr, Anna-Maija Juuso, Moussa Ouedraogo, and Juha Röning</i>	

FASES 2016

FASES I: Data Protection, Privacy Preservation and Discrimination Discovery

Privacy Preserving Computations for Viral Marketing: The Case of Rational Players	677
<i>Rica Gonen and Tamir Tassa</i>	

Protecting Sensitive Information in the Volatile Memory from Disclosure Attacks	687
<i>Stefanos Malliaros, Christoforos Ntantogian, and Christos Xenakis</i>	

FASES II: Economic Value of Personal Information

The Value of Online Users: Empirical Evaluation of the Price of Personalized Ads	694
<i>Miriam Marciel, Jose Gonzalez, Yonas Mitike Kassa, Roberto Gonzalez, and Mohamed Ahmed</i>	

Your Data in the Eyes of the Beholders: Design of a Unified Data Valuation Portal to Estimate Value of Personal Information from Market Perspective	701
<i>Yonas Mitike Kassa, Jose Gonzalez, Ángel Cuevas, Rubén Cuevas, Miriam Marciel, and Roberto González</i>	

FASES III: Novel Methods for Authentication, Identification and Certificates Issuance

Ensuring the Authenticity and Fidelity of Captured Photos Using Trusted Execution and Mobile Application Licensing Capabilities	706
<i>Kwstantinos Papadamou, Riginos Samaras, and Michael Sirivianos</i>	
FEBA: An Action-Based Feature Extraction Framework for Behavioural Identification and Authentication	715
<i>Luigi Stammati, Claudio Pisa, Tooska Dargahi, Alberto Caponi, and Giuseppe Bianchi</i>	
Automated Issuance of Digital Certificates through the Use of Federations	725
<i>Thaís Bardini Idalino, Marina Coelho, and Jean Everson Martina</i>	

SECPID 2016

SECPID I: Security and Privacy in the Cloud I

PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services	733
<i>Thomas Loruenser, Daniel Slamanig, Thomas Länger, and Henrich C. Pöhls</i>	
CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing	742
<i>Felix Hörandner, Stephan Krenn, Andrea Migliavacca, Florian Thiemer, and Bernd Zwattendorfer</i>	
Towards Secure Collaboration in Federated Cloud Environments	750
<i>Bojan Suzic and Andreas Reiter</i>	

SECPID II: Security and Privacy in the Cloud II

Cryptographically Enforced Four-Eyes Principle	760
<i>Arne Bilzhause, Manuel Huber, Henrich C. Pöhls, and Kai Samelin</i>	
Co-creating Security-and-Privacy-by-Design Systems	768
<i>Sauro Vicini, Francesco Alberti, Nicolás Notario, Alberto Crespo, Juan Ramón Troncoso Pastoriza, and Alberto Sanna</i>	
Tackling the Cloud Adoption Dilemma - A User Centric Concept to Control Cloud Migration Processes by Using Machine Learning Technologies	776
<i>Michael Diener, Leopold Blessing, and Nina Rappel</i>	

MUININ 2016

MUININ I

The Slandail Monitor: Real-Time Processing and Visualisation of Social Media Data for Emergency Management	786
<i>Xiubo Zhang, Stephen Kelly, and Khurshid Ahmad</i>	
Ensuring Security of Data and Information Flow in Emergency Response Decision Support	792
<i>Damian Jackson and Paul Hayes</i>	
Legal Implications of Using Social Media Data in Emergency Response	798
<i>Christian Berger, Paolo De Stefani, and Taiwo Oriola</i>	
Disaster-Related Public Speeches: The Role of Emotions	800
<i>Maria Spyropoulou and Khurshid Ahmad</i>	

MUININ II

The Application of Social Media Image Analysis to an Emergency Management System	805
<i>Min Jing, Bryan W. Scotney, Sonya A. Coleman, and Martin T. McGinnity</i>	
Computational, Communicative, and Legal Conditions for Using Social Media in Disaster Management in Germany	811
<i>Sabine Gründer-Fahrer, Christian Berger, Antje Schlaf, and Gerhard Heyer</i>	

SOCOTUD 2016

SOCOTUD I: Talks and Discussions on Recent Trends in User Involvement and Social Collaboration

Involving End Users into Collaborative Software Development: The Showcase of CloudTeams	821
<i>S. Franken, S. Kolvenbach, and W. Gräether</i>	
Social Analytics in an Enterprise Context: From Manufacturing to Software Development	827
<i>Evangelos Arvanitakis, Michael Petychakis, Evmorfia Biliri, Ariadni Michalitsi-Psarrou, Panagiotis Kokkinakos, Fenareti Lampathaki, and Dimitrios Askounis</i>	
SmartNet: Secure Content Sharing for Peer-to-Peer Smart Group Spaces	834
<i>Brian Greaves and Marijke Coetzee</i>	

SOCOTUD II: Demonstration, Talks, and Discussion on Social Collaboration in Software Development

Geographic Localization of an Anonymous Social Network Message Data Set	844
<i>Alexander Böhm, Benjamin Taubmann, and Hans P. Reiser</i>	
Using Crowdsourced and Anonymized Personas in the Requirements Elicitation and Software Development Phases of Software Engineering	851
<i>Iosif Alvertis, Dimitris Papaspyros, Sotiris Koussouris, Spyros Mouzakitis, and Dimitris Askounis</i>	
Author Index	857