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

Salzburg, Austria
31 August – 2 September 2016
Message from the ARES 2016 Program Committee Co-Chairs
ARES 2016 Organizing Committee
ARES 2016 Program Committee
Message from the ARES 2016 Workshop Chair
Message from the FARES 2016 Workshop Organizers
Message from the WSDF 2016 Workshop Organizers
WSDF 2016 Program Committee
Message from the IWSMA 2016 Workshop Organizers
IWSMA 2016 Program Committee
Message from the IWCC 2016 Workshop Organizers
IWCC 2016 Program Committee
Message from the SAW 2016 Workshop Organizers
SAW 2016 Program Committee
Message from the SecATM 2016 Workshop Organizers
SecATM 2016 Program Committee
Message from the ASSD 2016 Workshop Organizers
ASSD 2016 Program Committee
Message from the WMA 2016 Workshop Organizers
ARES Full Papers

ARES Full I: Best Paper Session
A Recommender-Based System for Assisting Non-technical Users in Managing Android Permissions

Arnaud Oglaza, Romain Laborde, Abdelmalek Benzekri, and François Barrère

No Need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large

Wilfried Mayer, Aaron Zauner, Martin Schmiedecker, and Markus Huber

Revisiting a Watermark-Based Detection Scheme to Handle Cyber-Physical Attacks

José Rubio-Hernán, Luca De Cicco, and Joaquín Garcia-Alfaro

ARES Full II: Cryptography
Byzantine Set-Union Consensus Using Efficient Set Reconciliation

Florian Dold and Christian Grothoff

k-Times Full Traceable Ring Signature

Xavier Bultel and Pascal Lafourcade
Towards Cycle-Accurate Emulation of Cortex-M Code to Detect Timing

Towards Cycle-Accurate Emulation of Cortex-M Code to Detect Timing

Side Channels ..................................................................................................................................................49
Johannes Bauer and Felix Freiling

ARES Full III: Network and Software Security

POTR: Practical On-the-Fly Rejection of Injected and Replayed 802.15.4 Frames ..................................................................................................................................................59
Konrad-Felix Krentz, Christoph Meinel, and Maxim Schnjakin

Stopping Amplified DNS DDoS Attacks through Distributed Query Rate Sharing ..................................................................................................................................................69
Saurabh Verma, Ali Hamieh, Jun Ho Huh, Henrik Holm,
Siva Raj Rajagopalan, Maciej Korczynski, and Nina Fefferman

HyperCrypt: Hypervisor-Based Encryption of Kernel and User Space ..................................................................................................................79
Johannes Götzfried, Nico Dörr, Ralph Palutke, and Tilo Müller

ARES Full IV: Privacy-Enhancing Technologies

Efficient and Privacy Preserving Third Party Auditing for a Distributed Storage System ..................................................................................................................................................88
Denise Demirel, Stephan Krenn, Thomas Lorünser, and Giulia Traverso

Introducing Proxy Voting to Helios ..................................................................................................................................................98
Oksana Kulyk, Karola Marky, Stephan Neumann, and Melanie Volkamer

ARES Full V: Applications

ARTIST: The Android Runtime Instrumentation Toolkit ..................................................................................................107
Lukas Dresel, Mykolai Protenko, and Tilo Müller

Development of an AUTOSAR Compliant Cryptographic Library on State-of-the-Art Automotive Grade Controllers ..................................................................................................................................................117
Pal-Stefan Murvay, Alexandru Matei, Cristina Solomon, and Bogdan Groza

Using Expert Systems to Statical Detect "Dynamic" Conflicts in XACML ..................................................................................................................................................127
Bernard Stepien and Amy Felty

ARES Full VI: Intrusion Detection and Incident Response

Selection of Mitigation Actions Based on Financial and Operational Impact Assessments ..................................................................................................................................................137
Gustavo Gonzalez Granadillo, Alexander Motzek, Joaquin Garcia-Alfaro, and Hervé Debar

A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow ..................................................................................................................................................147
Mehdi Nobakht, Vijay Sivaraman, and Roksana Boreli

Towards a CDS-based Intrusion Detection Deployment Scheme for Securing Industrial Wireless Sensor Networks ..................................................................................................................................................157
Lyes Bayou, Nora Cuppens-Boulahia, David Espès, and Frédéric Cuppen
ARES Short III: Cryptography

Energy Efficient Mutual Authentication and Key Agreement Scheme with Strong Anonymity Support for Secure Ubiquitous Roaming Services .............................................247
Prosanta Gope, Ruei-Hau Hsu, Jemin Lee, and Tony Q. S. Quek

Proviable User Authentication Scheme in Telecare Medicine Information System Using Elliptic Curve Cryptosystem ...............................................................253
Toan Thinh Truong, Duong Tien Phan, Minh Triet Tran, Anh Duc Duong, and Isao Echizen

Synchronous One Time Biometrics with Pattern Based Authentication .......................................................260
Patrick Lacharme and Christophe Rosenberger

V-DIFT: Vector-Based Dynamic Information Flow Tracking with Application to Locating Cryptographic Keys for Reverse Engineering ...........................................266
Antonio M. Espinoza, Jeffrey Knockel, Pedro Comesaña-Alfaro, and Jedidiah R. Crandall

ARES Short IV: Security Methods

Usable Privacy-Aware Logging for Unstructured Log Entries .................................................................272
Christof Rath

pwnPr3d: An Attack-Graph-Driven Probabilistic Threat-Modeling Approach .............................................278
Pontus Johnson, Alexandre Vernotte, Mathias Ekstedt, and Robert Lagerström

The Landscape of Domain Name Typosquatting: Techniques and Countermeasures .....................................284
Jeffrey Spaulding, Shambhu Upadhyaya, and Aziz Mohaisen

FARES 2016

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

Caller-Centrality: Identifying Telemarketers in a VoIP Network ............................................................290
Muhammad Ajmal Azad and Syed Khurram Rizvi

Collaborative Attribute Retrieval in Environment with Faulty Attribute Managers ........................................296
Mario Faiella, Fabio Martinelli, Paolo Mori, Andrea Saracino, and Mina Sheikhalishahi

Recognizing Time-Efficiently Local Botnet Infections - A Case Study .....................................................304
Tanja Heuer, Ina Schiering, Frank Klawonn, Alexander Gabel, and Martin Seeger

VoIP Profiler: Profiling Voice over IP User Communication Behavior .....................................................312
Sainath Batthalla, Mayank Swarnkar, Neminath Hubballi, and Maitreya Natu
WSDF 2016

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

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

IWSMA 2016

IWSMA I: International Workshop on Security of Mobile Applications
Notary-Assisted Certificate Pinning for Improved Security of Android Apps
Georg Merzdovnik, Damjan Buhov, Artemios G. Voyiatzis, and Edgar R. Weippl
Spotting the Malicious Moment: Characterizing Malware Behavior Using Dynamic Features
Alberto Ferrante, Eric Medvet, Francesco Mercaldo, Jelena Milosevic, and Corrado Aaron Visaggio

IWSMA II: International Workshop on Security of Mobile Applications
Lightweight Encryption for Smart Home
Sanaah Al Salami, Joonsang Baek, Khaled Salah, and Ernesto Damiani
Hand Dynamics for Behavioral User Authentication
Fuensanta Torres Garcia, Katharina Krombholz, Rudolf Mayer, and Edgar Weippl
IWCC 2016

IWCC I: International Workshop on Cyber Crime

Law Enforcement Access to Password Protected and/or Encrypted Mobile Data .................................................................................................................. 399

*Murdoch Watney*

Towards Digital Investigation in Virtual Networks: A Study of Challenges and Open Problems ........................................................................................................ 406

*Daniel Spiekermann and Tobias Eggendorfer*

Threat from Within: Case Studies of Insiders Who Committed Information Technology Sabotage ........................................................................................................ 414

*Jason W. Clark*

Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers ............................................................................................................ 423

*S. Kumar, L. Madhavan, M. Nagappan, and B. Sikdar*

SAW 2016

SAW I: International Software Assurance Workshop

Towards a Unified Secure Cloud Service Development and Deployment Life-Cycle ............................................................................................................................... 428

*Aleksandar Hudic, Matthias Flittner, Thomas Lorünser, Philipp M. Radl, and Roland Bless*

A Security Game Model for Remote Software Protection ............................................................................................................. 437

Nicola Basilico, Andrea Lanzi, and Mattia Monga

SPARER: Secure Cloud-Proof Storage for e-Health Scenarios ............................................................................................................. 444

Gabriela Gheorghe, Muhammad Rizwan Asghar, Jean Lancrenon, and Sankalp Ghatpande

SAW II: International Software Assurance Workshop

How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection ............................................................................................................. 454

*Nikhil Tripathi, Neminath Hubballi, and Yogendra Singh*

A Type System for Quantified Information-Flow Security in Java-Like Languages ............................................................................................................. 464

Gohar Shakoori, Mehran S. Fallah, and Zeinab Iranmanesh

On Analyzing Program Behavior under Fault Injection Attacks ............................................................................................................. 474

Jakub Breier
SAW III: International Software Assurance Workshop
Authentication in the Context of E-Participation: Current Practice,
Challenges and Recommendations ........................................................................................................480
Maria Leitner and Arndt Bonitz

SecATM 2016

SecATM I: ATM Security Research and Development
Air Traffic Management Security Research in SESAR .............................................................................486
John Hird, Martin Hawley, and Chris Machin
Claudio Porretti, Raoul Lahaije, and Denis Kolev
CTRL_S - A Security Tool for SESAR's Design-In Security Approach ..................................................499
Karol Gotz, Martin Hawley, Chris Machin, and John Hird

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

SecATM III: Testing and Validation
Security Testing with Controller-Pilot Data Link Communications ..................................................................526
Doris Di Marco, Alessandro Manzo, Marco Ivaldi, and John Hird
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
Patrizia Montefusco, Rosana Casar, Rainer Koelle, and Tim H. Stelkens-Kobsch

ASSD 2016

ASSD I: Secure DevOps
SecDevOps: Is It a Marketing Buzzword? - Mapping Research on Security in DevOps .................................................................542
Vaishnavi Mohan and Lotfi Ben Othmane
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
   Tosin Daniel Oyetoyan, Daniela Soares Cruzes, and Martin Gilje Jaatun

   Kalle Rindell, Sami Hyrynsalmi, and Ville Leppänen

Towards Effective Security Assurance for Incremental Software Development the Case of Zen Cart Application .......................................................... 564
   Lotfi Ben Othmane and Azmat Ali

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

Misuse, Abuse and Reuse: Economic Utility Functions for Characterising Security Requirements .......................................................... 572
   Chad Heitzenrater and Andrew Simpson

Agile Team Members Perceptions on Non-functional Testing: Influencing Factors from an Empirical Study .......................................................... 582
   Cristina Rosa Camacho, Sabrina Marczak, and Daniela S. Cruzes

WMA 2016

WMA I: International Workshop on Malware Analysis

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

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
   Enrico Mariconti, Jeremiah Onaolapo, Gordon Ross, and Gianluca Stringhini

Exploring the Usage of Topic Modeling for Android Malware Static Analysis .......................................................... 609
   Eric Medvet and Francesco Mercaldo

Classification of Short Messages Initiated by Mobile Malware .......................................................... 618
   Marian Kühlner and Ulrike Meyer

WMA III: International Workshop on Malware Analysis

Ransomware Inside Out .......................................................... 628
   Francesco Mercaldo, Vittoria Nardone, and Antonella Santone
Detecting Packed Executable File: Supervised or Anomaly Detection
Method? .................................................................638

Neminath Hubballi and Himanshu Dogra

ISPM 2016

ISPM I: Challenges, Threats and Solutions
The Perfect Storm: The Privacy Paradox and the Internet-of-Things ..................................................644

Meredydd Williams, Jason R. C. Nurse, and Sadie Creese

ISPM II: Models and Communication
Privacy Impact Assessment Template for Provenance .................................................................653

Jenni Reuben, Leonardo A. Martucci, Simone Fischer-Hübner,
Heather S. Packer, Hans Hedbom, and Luc Moreau

Major Challenges in Structuring and Institutionalizing
CERT-Communication .................................................................661

Otto Hellwig, Gerald Quirchmayr, Edith Huber, Gernot Goluch, Franz Vock,
and Bettina Pospisil

Towards a Complex Systems Approach to Legal and Economic Impact
Analysis of Critical Infrastructures .................................................................668

Thomas Schaberreiter, Gerald Quirchmayr, Anna-Maija Juuso,
Moussa Ouedraogo, and Juha Röning

FASES 2016

FASES I: Data Protection, Privacy Preservation and Discrimination Discovery
Privacy Preserving Computations for Viral Marketing: The Case of Rational
Players .................................................................677

Rica Gonen and Tamir Tassa

Protecting Sensitive Information in the Volatile Memory from Disclosure
Attacks .................................................................687

Stefanos Malliaros, Christoforos Ntantogian, and Christos Xenakis

FASES II: Economic Value of Personal Information
The Value of Online Users: Empirical Evaluation of the Price
of Personalized Ads .................................................................694

Miriam Marciel, Jose Gonzalez, Yonas Mitike Kassa, Roberto Gonzalez,
and Mohamed Ahmed

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

Yonas Mitike Kassa, Jose Gonzalez, Ángel Cuevas, Rubén Cuevas,
Miriam Marciel, and Roberto González
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
  Kwstantinos Papadamou, Riginos Samaras, and Michael Sirivianos

FEBA: An Action-Based Feature Extraction Framework for Behavioural Identification and Authentication ............................................................................................................ 715
  Luigi Stammati, Claudio Pisa, Tooska Dargahi, Alberto Caponi, and Giuseppe Bianchi

Automated Issuance of Digital Certificates through the Use of Federations ........................................ 725
  Thais Bardini Idalino, Marina Coelho, and Jean Everson Martina

SECPID 2016

SECPID I: Security and Privacy in the Cloud I

PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services ................................................................. 733
  Thomas Loruenser, Daniel Slamanig, Thomas Länger, and Henrich C. Pöhls

CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing ................................................................. 742
  Felix Hörandner, Stephan Krenn, Andrea Migliavacca, Florian Thiemer, and Bernd Zwattendorfer

Towards Secure Collaboration in Federated Cloud Environments .................................................................................. 750
  Bojan Suzic and Andreas Reiter

SECPID II: Security and Privacy in the Cloud II

Cryptographically Enforced Four-Eyes Principle ................................................................................................. 760
  Arne Bilzhause, Manuel Huber, Henrich C. Pöhls, and Kai Samelin

Co-creating Security-and-Privacy-by-Design Systems ................................................................................................. 768
  Sauro Vicini, Francesco Alberti, Nicolás Notario, Alberto Crespo, Juan Ramón Troncoso Pastoriza, and Alberto Sanna

Tackling the Cloud Adoption Dilemma - A User Centric Concept to Control Cloud Migration Processes by Using Machine Learning Technologies ............................................. 776
  Michael Diener, Leopold Blessing, and Nina Rappel

MUININ 2016
## MUININ I

The Slandail Monitor: Real-Time Processing and Visualisation of Social Media Data for Emergency Management .......................................................... 786

*Xiubo Zhang, Stephen Kelly, and Khurshid Ahmad*

Ensuring Security of Data and Information Flow in Emergency Response Decision Support ........................................................................................................... 792

*Damian Jackson and Paul Hayes*

Legal Implications of Using Social Media Data in Emergency Response .................................................................................................................. 798

*Christian Berger, Paolo De Stefani, and Taiwo Oriola*

Disaster-Related Public Speeches: The Role of Emotions .................................................. 800

*Maria Spyropoulou and Khurshid Ahmad*

## MUININ II

The Application of Social Media Image Analysis to an Emergency Management System ........................................................................................................... 805

*Min Jing, Bryan W. Scotney, Sonya A. Coleman, and Martin T. McGinnity*

Computational, Communicative, and Legal Conditions for Using Social Media in Disaster Management in Germany ........................................................................ 811

*Sabine Gründer-Fahrer, Christian Berger, Antje Schlaf, and Gerhard Heyer*

## 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

*S. Franken, S. Kolvenbach, and W. Gräether*

Social Analytics in an Enterprise Context: From Manufacturing to Software Development ........................................................................................................... 827

*Evangelos Arvanitakis, Michael Petychakis, Evmorfia Biliri, Ariadni Michalitsi-Psarrou, Panagiotis Kokkinakos, Fenareti Lampathaki, and Dimitrios Askounis*

SmartNet: Secure Content Sharing for Peer-to-Peer Smart Group Spaces .................................................................................................................. 834

*Brian Greaves and Marijke Coetzee*
SOCOTUD II: Demonstration, Talks, and Discussion on Social Collaboration in Software Development

Geographic Localization of an Anonymous Social Network Message Data
Set ......................................................................................................................................................844

Alexander Böhm, Benjamin Taubmann, and Hans P. Reiser

Using Crowdsourced and Anonymized Personas in the Requirements Elicitation and Software Development Phases of Software Engineering ........................................851

Iosif Alvertis, Dimitris Papaspyros, Sotiris Koussouris, Spyros Mouzakitis,
and Dimitris Askounis

Author Index ......................................................................................................................................857