

# **2015 10th International Conference on Availability, Reliability and Security (ARES 2015)**

**Toulouse, France  
24 – 27 August 2015**



**IEEE Catalog Number: CFP1539A-POD  
ISBN: 978-1-4673-6591-8**

# 2015 10th International Conference on Availability, Reliability and Security

## ARES 2015 Table of Contents

Welcome Message from ARES Program Committee	
Co-Chair and General Chair .....	xiv
ARES 2015 Program Committee and Local Organizing Committee .....	xv
Welcome Message from the ARES 2015 Workshop Chair .....	xviii
Welcome Message from the FARES 2015 Workshop Organizers .....	xix
Welcome Message from the WSDF 2015 Workshop Organizers .....	xx
WSDF 2015 Program Committee .....	xxi
Welcome Message from the IWSMA 2015 Workshop Organizers .....	xxii
IWSMA 2015 Program Committee .....	xxiii
Welcome Message from the IWCC 2015 Workshop Organizers .....	xxiv
IWCC 2015 Program Committee .....	xxv
Welcome Message from the SAW 2015 Workshop Organizers .....	xxvi
SAW 2015 Program Committee .....	xxvii
Welcome Message from the ASSD 2015 Workshop Organizers .....	xxviii
ASSD 2015 Program Committee .....	xxix
Welcome Message from the WCSF 2015 Workshop Organizers .....	xxx
WCSF 2015 Program Committee .....	xxxi
Welcome Message from the MFSec 2015 Workshop Organizers .....	xxxii
MFSec 2015 Program Committee .....	xxxiii
Welcome Message from the ARES EU Projects Symposium .....	xxxiv
Welcome Message from the AU2EU 2015 Workshop Organizers .....	xxxv
AU2EU 2015 Program Committee .....	xxxvi

<b>Welcome Message from the FCCT 2015 Workshop</b>	
<b>Organizers</b> .....	xxxvii
<b>FCCT 2015 Program Committee</b> .....	xxxviii
<b>Welcome Message from the STAM 2015 Workshop</b>	
<b>Organizers</b> .....	xxxix
<b>STAM 2015 Program Committee</b> .....	xl

---

## **10th International Conference on Availability, Reliability and Security: ARES 2015**

### **Full Papers**

#### **ARES Full I: Best Paper Session**

Structural Weaknesses in the Open Smart Grid Protocol .....	1
<i>Klaus Kursawe and Christiane Peters</i>	
A Novel Security-Enhanced Agile Software Development Process Applied in an Industrial Setting .....	11
<i>Dejan Baca, Martin Boldt, Bengt Carlsson, and Andreas Jacobsson</i>	
Optimizing IT Service Costs with Respect to the Availability Service Level Objective .....	20
<i>Sascha Bosse, Matthias Splieth, and Klaus Turowski</i>	

#### **ARES Full II: Identity and Privacy**

PALPAS—PAssword Less PAssword Synchronization .....	30
<i>Moritz Horsch, Andreas Hülsing, and Johannes Buchmann</i>	
Advanced Identity and Access Policy Management Using Contextual Data .....	40
<i>Matthias Hummer, Michael Kunz, Michael Netter, Ludwig Fuchs, and Günther Pernul</i>	
Publicly Verifiable Private Aggregation of Time-Series Data .....	50
<i>Bence Gábor Bakondi, Andreas Peter, Maarten Everts, Pieter Hartel, and Willem Jonker</i>	

#### **ARES Full III: Networks and Protocols**

Accountable Redactable Signatures .....	60
<i>Henrich C. Pöhls and Kai Samelin</i>	
The Role and Security of Firewalls in IaaS Cloud Computing .....	70
<i>Jordan Cropper, Johanna Ullrich, Peter Frühwirt, and Edgar Weippl</i>	
Empirical Evaluation of the A3 Environment: Evaluating Defenses Against Zero-Day Attacks .....	80
<i>Shane S. Clark, Aaron Paulos, Brett Benyo, Partha Pal, and Richard Schantz</i>	

#### **ARES Full IV: Software Security**

Uncovering Use-After-Free Conditions in Compiled Code .....	90
<i>David Dewey, Bradley Reaves, and Patrick Traynor</i>	
All-Solution Satisfiability Modulo Theories: Applications, Algorithms and Benchmarks .....	100
<i>Quoc-Sang Phan and Pasquale Malacaria</i>	

Fair Fingerprinting Protocol for Attesting Software Misuses .....	110
<i>Raphael C.S. Machado, Davidson R. Boccardo, Vinícius G. Pereira de Sá, and Jayme L. Szwarcfiter</i>	

### **ARES Full V: Mobile Security and Cyber Physical Systems**

A Lightweight Framework for Cold Boot Based Forensics on Mobile Devices .....	120
<i>Benjamin Taubmann, Manuel Huber, Sascha Wessel, Lukas Heim, Hans Peter Reiser, and Georg Sigl</i>	
Dynamic Self-Protection and Tamperproofing for Android Apps Using Native Code .....	129
<i>Mykola Protsenko, Sebastien Kreuter, and Tilo Müller</i>	
Don't Brick Your Car: Firmware Confidentiality and Rollback for Vehicles .....	139
<i>Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram, and Keith Mayes</i>	

### **ARES Full VI: Security Management**

Modeling Fraud Prevention of Online Services Using Incident Response Trees and Value at Risk .....	149
<i>Dan Gorton</i>	
The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001 .....	159
<i>Bahareh Shojaie, Hannes Federrath, and Iman Saberi</i>	

### **Short Papers**

#### **ARES Short I: Network and Probing**

On the Isomorphism of Network Access Control Lists .....	168
<i>Malek Belhaouane, Joaquin Garcia-Alfaro, and Hervé Debar</i>	
Trust me, I'm a Root CA! Analyzing SSL Root CAs in Modern Browsers and Operating Systems .....	174
<i>Tariq Fadaei, Sebastian Schrittwieser, Peter Kieseberg, and Martin Mulazzani</i>	
A Time Series Approach for Inferring Orchestrated Probing Campaigns by Analyzing Darknet Traffic .....	180
<i>Elias Bou-Harb, Mourad Debbabi, and Chadi Assi</i>	
On Reconnaissance with IPv6: A Pattern-Based Scanning Approach .....	186
<i>Johanna Ullrich, Peter Kieseberg, Katharina Krombholz, and Edgar Weippl</i>	

#### **ARES Short II: Hardware and Physical Layer Security**

Hardware Security Evaluation Using Assurance Case Models .....	193
<i>Henrique Kawakami, Roberto Gallo, Ricardo Dahab, and Erick Nascimento</i>	
Physically Secure Code and Data Storage in Autonomously Booting Systems .....	199
<i>Johannes Götzfried, Johannes Hampel, and Tilo Müller</i>	
Error/Intrusion Target Identification on the Physical Layer over a BICM Scheme .....	205
<i>Sihem Chaabouni and Amel Meddeb-Makhlouf</i>	
Towards Abuse Detection and Prevention in IaaS Cloud Computing .....	211
<i>Jens Lindemann</i>	

### **ARES Short III: Social Networks, Voting and Usable Security**

A Model Implementing Certified Reputation and Its Application to TripAdvisor .....	218
<i>Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera</i>	
Efficiency Evaluation of Cryptographic Protocols for Boardroom Voting .....	224
<i>Oksana Kulyk, Stephan Neumann, Jurlind Budurushi, Melanie Volkamer, Rolf Haenni, Reto Koenig, and Philemon von Bergen</i>	
QR Code Security—How Secure and Usable Apps Can Protect Users Against Malicious QR Codes .....	230
<i>Katharina Krombholz, Peter Frühwirt, Thomas Rieder, Ioannis Kapsalis, Johanna Ullrich, and Edgar Weippl</i>	
Event Prediction with Community Leaders .....	238
<i>Jun Pang and Yang Zhang</i>	

### **The 10th International Workshop on Frontiers in Availability, Reliability and Security: FARES 2015**

#### **FARES I: Monitoring and Identification**

Privacy and Trust in Smart Camera Sensor Networks .....	244
<i>Michael Loughlin and Asma Adnane</i>	
Towards the Forensic Identification and Investigation of Cloud Hosted Servers through Non-Invasive Wiretaps .....	249
<i>Hessel Schut, Mark Scanlon, Jason Farina, and Nhien-An Le-Khac</i>	
Security Monitoring of HTTP Traffic Using Extended Flows .....	258
<i>Martin Husák, Petr Velan, and Jan Vykopal</i>	

#### **FARES II: Cryptography and Resilience**

Towards a Process-Centered Resilience Framework .....	266
<i>Richard M. Zahoransky, Christian Brenig, and Thomas Koslowski</i>	
Complexity Estimates of a SHA-1 Near-Collision Attack for GPU and FPGA .....	274
<i>Jürgen Fuß, Stefan Gradinger, Bernhard Greslehner-Nimmervoll, and Robert Kolmhofer</i>	
Impacts of Tourist Accommodations as Temporal Shelter on Evacuee Overflow for the Reassignment of Shelters Jurisdiction .....	281
<i>Yu Ichifuji, Noriaki Koide, and Noboru Sonehara</i>	

### **The Eighth International Workshop on Digital Forensics: WSDF 2015**

Cold Boot Attacks on DDR2 and DDR3 SDRAM .....	287
<i>Simon Lindenlauf, Hans Höfken, and Marko Schuba</i>	
Behavioural Evidence Analysis Applied to Digital Forensics: An Empirical Analysis of Child Pornography Cases Using P2P Networks .....	293
<i>Noora Al Mutawa, Joanne Bryce, Virginia N.L. Franqueira, and Andrew Marrington</i>	
Watch What You Wear: Preliminary Forensic Analysis of Smart Watches .....	303
<i>Ibrahim Baggili, Jeff Oduro, Kyle Anthony, Frank Breitingner, and Glenn McGee</i>	
Challenges of Data Provenance for Cloud Forensic Investigations .....	312
<i>Victoria M. Katilu, Virginia N.L. Franqueira, and Olga Angelopoulou</i>	

## **The Fourth International Workshop on Security of Mobile Applications: IWSMA 2015**

### **IWSMA I: Android Security**

Composition-Malware: Building Android Malware at Run Time .....	318
<i>Gerardo Canfora, Francesco Mercaldo, Giovanni Moriano, and Corrado Aaron Visaggio</i>	
Network Security Challenges in Android Applications .....	327
<i>Damjan Buhov, Markus Huber, Georg Merzdovnik, Edgar Weippl, and Vesna Dimitrova</i>	
Effectiveness of Opcode ngrams for Detection of Multi Family Android Malware .....	333
<i>Gerardo Canfora, Andrea De Lorenzo, Eric Medvet, Francesco Mercaldo, and Corrado Aaron Visaggio</i>	

### **IWSMA II: Networks Security**

A Model for Specification and Validation of a Trust Management Based Security Scheme in a MANET Environment .....	341
<i>Aida Ben Chehida Douss, Ryma Abassi, and Sihem Guemara El Fatmi</i>	
Risk Assessment of Public Safety and Security Mobile Service .....	351
<i>Matti J. Peltola and Pekka Kekolahti</i>	
Trust Negotiation Based Approach to Enforce MANET Routing Security .....	360
<i>Aida Ben Chehida Douss, Samiha Ayed, Ryma Abassi, Nora Cuppens, and Sihem Ghemara El Fatmi</i>	

## **International Workshop on Cyber Crime: IWCC 2015**

### **IWCC I: Cyber Crime Techniques and Prevention**

Intensifying State Surveillance of Electronic Communications: A Legal Solution in Addressing Extremism or Not? .....	367
<i>Murdoch Watney</i>	
Malicious Insiders with Ties to the Internet Underground Community .....	374
<i>Jason W. Clark, Matt Collins, and Jeremy Strozer</i>	
An Empirical Study of Click Fraud in Mobile Advertising Networks .....	382
<i>Geumhwan Cho, Junsung Cho, Youngbae Song, and Hyoungshick Kim</i>	
Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting .....	389
<i>Martin Husák, Milan Čermák, Tomáš Jirsík, and Pavel Čeleda</i>	

### **IWCC II: Cyber Crime Techniques and Prevention**

Deploying Honeypots and Honeynets: Issue of Privacy .....	397
<i>Pavol Sokol, Martin Husak, and František Lipták</i>	
Gradually Improving the Forensic Process .....	404
<i>Sebastian Neuner, Martin Mulazzani, Sebastian Schrittwieser, and Edgar Weippl</i>	
A Landmark Calibration Based IP Geolocation Approach .....	411
<i>Jingning Chen, Fenlin Liu, Xiangyang Luo, Fan Zhao, and Guang Zhu</i>	
Markov Process Based Retrieval for Encrypted JPEG Images .....	417
<i>Hang Cheng, Xinpeng Zhang, Jiang Yu, and Fengyong Li</i>	

### **IWCC III: Information Hiding I**

Countermeasures for Covert Channel-Internal Control Protocols .....	422
<i>Jaspreet Kaur, Steffen Wendzel, and Michael Meier</i>	
Novel Method of Hiding Information in IP Telephony Using Pitch Approximation .....	429
<i>Artur Janicki</i>	
Steg Blocks: Ensuring Perfect Undetectability of Network Steganography .....	436
<i>Wojciech Frączek and Krzysztof Szczypiorski</i>	
Using Facebook for Image Steganography .....	442
<i>Jason Hiney, Tejas Dakve, Krzysztof Szczypiorski, and Kris Gaj</i>	

### **IWCC IV: Information Hiding II**

Color Image Steganalysis Using Correlations between RGB Channels .....	448
<i>Hasan Abdulrahman, Marc Chaumont, Philippe Montesinos, and Baptiste Magnier</i>	
Steganalysis of Low Bit-Rate Speech Based on Statistic Characteristics of Pulse Positions .....	455
<i>Hui Tian, Yanpeng Wu, Yongfeng Huang, Jin Liu, Yonghong Chen, Tian Wang, and Yiqiao Cai</i>	
A JPEG-Compression Resistant Adaptive Steganography Based on Relative Relationship between DCT Coefficients .....	461
<i>Yi Zhang, Xiangyang Luo, Chunfang Yang, Dengpan Ye, and Fenlin Liu</i>	

## **The Second International Workshop on Software Assurance: SAW 2015**

### **SAW I: Security Design and Validation**

How Much Cloud Can You Handle? .....	467
<i>Martin Gilje Jaatun and Inger Anne Tøndel</i>	
Generation of Local and Expected Behaviors of a Smart Card Application to Detect Software Anomaly .....	474
<i>Germain Jolly, Baptiste Hemery, and Christophe Rosenberger</i>	
Towards a CERT-Communication Model as Basis to Software Assurance .....	481
<i>Otto Hellwig, Gerald Quirchmayr, Edith Huber, Timo Mischitz, and Markus Huber</i>	
Securing Web Applications with Better "Patches": An Architectural Approach for Systematic Input Validation with Security Patterns .....	486
<i>Jung-Woo Sohn and Jungwoo Ryoo</i>	

### **SAW II: Software Testing and Assurance**

Personal Agent for Services in ITS .....	493
<i>Shinsaku Kiyomoto, Toru Nakamura, Haruo Takasaki, and Tatsuhiko Hirabayashi</i>	
Towards Black Box Testing of Android Apps .....	501
<i>Yury Zhauniarovich, Anton Philippov, Olga Gadyatskaya, Bruno Crispo, and Fabio Massacci</i>	
An Open Source Code Analyzer and Reviewer (OSCAR) Framework .....	511
<i>Simon Tjoa, Patrick Kochberger, Christoph Malin, and Andreas Schmoll</i>	

A Performance Evaluation of Hash Functions for IP Reputation Lookup Using Bloom Filters .....	516
<i>Marc Antoine Gosselin-Lavigne, Hugo Gonzalez, Natalia Stakhanova, and Ali A. Ghorbani</i>	

## **The First International Workshop on Agile Secure Software Development: ASSD 2015**

### **ASSD I: Experiences in Agile Development of Secure software**

Independent Security Testing on Agile Software Development: A Case Study in a Software Company .....	522
<i>Jesús Chóliz, Julián Vilas, and José Moreira</i>	
Incremental Development of RBAC-Controlled E-Marking System Using the B Method .....	532
<i>Nasser Al-Hadhrami, Benjamin Aziz, Shantanu Sardesai, and Lotfi ben Othmane</i>	

### **ASSD II: Assessment of Research on Agile Development of Secure software**

Literature Review of the Challenges of Developing Secure Software Using the Agile Approach .....	540
<i>Hela Oueslati, Mohammad Masudur Rahman, and Lotfi ben Othmane</i>	
Method Selection and Tailoring for Agile Threat Assessment and Mitigation .....	548
<i>Stephan Renatus, Clemens Teichmann, and Jörn Eichler</i>	

## **The International Workshop on Cloud Security and Forensics: WCSF 2015**

Overview of the Forensic Investigation of Cloud Services .....	556
<i>Jason Farina, Mark Scanlon, Nhien-An Le-Khac, and M-Tahar Kechadi</i>	
Advanced Attribute-Based Key Management for Mobile Devices in Hybrid Clouds .....	566
<i>Jaemin Park, Eunchan Kim, Sungjin Park, and Cheoloh Kang</i>	
Enabling Constraints and Dynamic Preventive Access Control Policy Enforcement in the Cloud .....	576
<i>Somchart Fugkeaw and Hiroyuki Sato</i>	
Evaluation of a Sector-Hash Based Rapid File Detection Method for Monitoring Infrastructure-as-a-Service Cloud Platforms .....	584
<i>Manabu Hirano, Hayate Takase, and Koki Yoshida</i>	

## **International Workshop on Multimedia Forensics and Security: MFSec 2015**

### **MFSec I: Web and Social Media Data Analytics for Privacy Awareness and terrorist-related Content identification**

PScore: A Framework for Enhancing Privacy Awareness in Online Social Networks .....	592
<i>Georgios Petkos, Symeon Papadopoulos, and Yiannis Kompatsiaris</i>	
A Framework for the Discovery, Analysis, and Retrieval of Multimedia Homemade Explosives Information on the Web .....	601
<i>Theodora Tsirikika, George Kalpakis, Stefanos Vrochidis, Ioannis Kompatsiaris, Iraklis Paraskakis, Isaak Kavasidis, Jonathan Middleton, and Una Williamson</i>	



## **MFSec II: Forensic Analysis of Audiovisual data**

Video Spatio-Temporal Filtering Based on Cameras and Target Objects	
Trajectories—Videosurveillance Forensic Framework .....	611
<i>Dana Codreanu, Andre Peninou, and Florence Sedes</i>	
Image Watermarking with Biometric Data for Copyright Protection .....	618
<i>Morgan Barbier, Jean-Marie Le Bars, and Christophe Rosenberger</i>	
AnonCall: Making Anonymous Cellular Phone Calls .....	626
<i>Eric Chan-Tin</i>	
Concept Detection in Multimedia Web Resources About Home Made Explosives .....	632
<i>George Kalpakis, Theodora Tsirikka, Foteini Markatopoulou, Nikiforos Pittaras, Stefanos Vrochidis, Vasileios Mezaris, Ioannis Patras, and Ioannis Kompatsiaris</i>	

## **Workshop on Security and Privacy in Cloud-Based Applications: Au2EU 2015**

A Secure Integrated Platform for Rapidly Formed Multiorganisation Collaborations .....	642
<i>John Zic, Nerolie Oakes, Dongxi Liu, Jane Li, Chen Wang, and Shiping Chen</i>	
Cross-Domain Attribute Conversion for Authentication and Authorization .....	652
<i>Stefan Thaler, Jerry Den Hartog, Dhouha Ayed, Dieter Sommer, and Michael Hitchens</i>	
Nomad: A Framework for Developing Mission-Critical Cloud-Based Applications .....	660
<i>Mamadou H. Diallo, Michael August, Roger Hallman, Megan Kline, Henry Au, and Vic Beach</i>	
The Measurement of Data Locations in the Cloud .....	670
<i>Bernd Jaeger, Reiner Kraft, Sebastian Luhn, Annika Selzer, and Ulrich Waldmann</i>	
Virtual Machine Introspection: Techniques and Applications .....	676
<i>Yacine Hebbal, Sylvie Laniepce, and Jean-Marc Menaud</i>	

## **The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism: FCCT 2015**

Comprehensive Approach to Increase Cyber Security and Resilience .....	686
<i>Michał Choraś, Rafał Kozik, Maria Pilar Torres Bruna, Artsiom Yautsiukhin, Andrew Churchill, Iwona Maciejewska, Irene Eguinoa, and Adel Jomni</i>	
Integrating Human Behavior Into the Development of Future Cyberterrorism Scenarios .....	693
<i>Max Kilger</i>	
2020 Cybercrime Economic Costs: No Measure No Solution .....	701
<i>Jart Armin, Bryn Thompson, Davide Ariu, Giorgio Giacinto, Fabio Roli, and Piotr Kijewski</i>	
0-Day Vulnerabilities and Cybercrime .....	711
<i>Jart Armin, Paolo Foti, and Marco Cremonini</i>	
Yet Another Cybersecurity Roadmapping Methodology .....	719
<i>Davide Ariu, Luca Didaci, Giorgio Fumera, Enrico Frumento, Federica Freschi, Giorgio Giacinto, and Fabio Roli</i>	

# **The First International Workshop on Security Testing and Monitoring: STAM 2015**

## **STAM I: Security Testing and Monitoring Solutions**

TEAR: A Multi-purpose Formal Language Specification for TEsting at Runtime .....	727
<i>Jorge López, Stephane Maag, and Gerardo Morales</i>	
An Active Testing Tool for Security Testing of Distributed Systems .....	735
<i>Mohamed H.E. Aouadi, Khalifa Toumi, and Ana Cavalli</i>	

## **STAM II: Security in Virtualized and Cloud Environments**

Monitoring and Securing New Functions Deployed in a Virtualized Networking Environment .....	741
<i>Bertrand Mathieu, Guillaume Doyen, Wissam Mallouli, Thomas Silverston, Olivier Bettan, François-Xavier Aguessy, Thibault Cholez, Abdelkader Lahmadi, Patrick Truong, and Edgardo Montes de Oca</i>	
Security Monitoring in the Cloud: An SLA-Based Approach .....	749
<i>Valentina Casola, Alessandra De Benedictis, and Massimiliano Rak</i>	
<b>Author Index</b> .....	756