2012 Seventh International Conference on Availability, Reliability and Security

(ARES 2012)

Prague, Czech Republic
20 – 24 August 2012
The Seventh International Conference on Availability, Reliability, and Security (ARES 2012)

Full Papers

Security as Quality Property

Analyses of Two End-User Software Vulnerability Exposure Metrics .................................................................1
  Jason L. Wright, Miles McQueen, and Lawrence Wellman

An Adaptive Risk Control and Security Management for Embedded Real-Time System .........................................11
  Yue Ma, Wei Jiang, Nan Sang, and Ziguo Zhong
Using Linear Support Vector Machines to Solve the Asymmetric Comparison-Based Fault Diagnosis Problem .............................................................. 18
*Mourad Elhadef*

**Aspects of Privacy**

*Stanislaus Stelle, Mark Manulis, and Matthias Hollick*

On Measuring the Parasitic Backscatter of Sensor-Enabled UHF RFID Tags .............................................................................................. 38
*Thomas Pias and Christian Maiherhofer*

Veto-based Malware Detection .................................................................................................................................................. 47
*Raja Khurram Shahzad and Niklas Lavesson*

**Cryptography**

Efficient Generic Construction of Forward-Secure Identity-Based Signature ........................................................................................... 55
*Noura Al Ebri, Joonsang Baek, Abdulhadi Shoufan, and Quang Hieu Vu*

From Computationally-proved Protocol Specifications to Implementations ............................................................................................ 65
*David Cadé and Bruno Blanchet*

Oblivious and Fair Server-Aided Two-Party Computation ................................................................................................................. 75
*Amir Herzberg and Haya Shulman*

**Privacy Enhancing Technologies**

A Group Signature Based Electronic Toll Pricing System ......................................................................................................................... 85
*Xihui Chen, Gabriele Lenzini, Souke Mauw, and Jun Pang*

Anonymous Communication by Branch-and-Bound .......................................................................................................................... 94
*Stefan Rass, Peter Schartner, Raphael Wigoutschnigg, and Christian Kollmitzer*

An Analysis of Implemented and Desirable Settings for Identity Management on Social Networking Sites .................................................. 103
*Moritz Riesner, Michael Netter, and Günther Pernul*

**Authorization and Authentication**

An Approach to Bridge the Gap between Role Mining and Role Engineering via Migration Guides ................................................................. 113
*Anne Baumgrass and Mark Strembeck*

Towards Automated Assistance for Mined Roles Analysis in Role Mining Applications ........................................................................ 123
*Safaà Hachana, Frédéric Cuppens, Nora Cuppens-Boulahia, and Joaquin Garcia-Alfaro*

A Coordination-Driven Authorization Framework for Space Containers .............................................................................................. 133
*Stefan Craß, Tobias Dönz, Gerson Joskowicz, and Eva Kühn*
Short Papers

Software Security
RIM: A Method to Defend from JIT Spraying Attack ................................................................. 143
  Rui Wu, Ping Chen, Bing Mao, and Li Xie

Building a Flexible Service Architecture for User Controlled Hybrid Clouds .................................................. 149
  Anja Strunk, Marc Mosch, Stephan Groß, Yvonne Thoß, and Alexander Schill

Towards a Holistic Information Security Governance Framework for SOA .................................................. 155
  Marijke Coetzee

Security and Usability
An Algorithm for Compression of XACML Access Control Policy Sets by Recursive Subsumption ................................................................. 161
  Bernard Stepien, Stan Matwin, and Amy Felty

E-mail Classification Using Social Network Information ................................................................. 168
  Anton Borg and Niklas Lavesson

Two-Pronged Phish Snagging ............................................................................................................... 174
  Rakesh Verma, Narasimha Shashidhar, and Nabil Hossain

Security in Electronic Services and Mobile Services
Civitas and the Real World: Problems and Solutions from a Practical Point of View .................................................. 180
  Stephan Neumann and Melanie Volkamer

Understanding the Development Trends of Electronic Voting Systems .................................................. 186
  Ali Fawzi Najm Al-Shammari, Adolfo Villafiorita, and Komminist Weldemariam

Secure Mobile Data Collection Systems for Low-Budget Settings .................................................. 196
  F. Mancini, S. Gejibo, K.A. Mughal, R.A.B. Valvik, and J. Klungsøy

Security Control
Dynamic DNS Update Security, Based on Cryptographically Generated Addresses and ID-Based Cryptography, in an IPv6 Autoconfiguration Context .................................................. 206
  Jean-Michel Combes, Ghada Arfaoui, and Maryline Laurent

Enforcing Access Control in Virtual Organizations Using Hierarchical Attribute-Based Encryption .................................................. 212
  Muhammad Asim, Tanya Ignatenko, Milan Petkovic, Daniel Trivellato, and Nicola Zannone

Boosting Logical Attack Graph for Efficient Security Control .................................................. 218
  Zonghua Zhang and Shuzhen Wang

High Level Model of Control Flow Attacks for Smart Card Functional Security .................................................. 224
  Pascal Berthemé, Karine Heydemann, X. Kauffmann-Tourkestansky, and Jean-Francois Lalande
Security Studies

Federated Identity Management Challenges ................................................................. Jostein Jensen

An Empirical Study on Design Diversity of Functionally Equivalent Web Services ......................................................... Amanda S. Nascimento, Fernando Castor, Cecilia M.F. Rubira, and Rachel Burrows

Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation Kristian Beckers, Stephan Faßbender, Maritta Heisel, and Holger Schmidt

Network Analysis and Security

A Personalized Whitelist Approach for Phishing Webpage Detection .......................................................... A. Belabed, E. Aïmeur, and A. Chikh

Model-Based Digit Analysis for Fraud Detection Overcomes Limitations of Benford Analysis ................................................ Christian Winter, Markus Schneider, and York Yannikos

Antidotes for DNS Poisoning by Off-Path Adversaries ................................................ Amir Herzberg and Haya Shulman

Cloud Security and Analysis

Classic Replication Techniques on the Cloud ........................................................................................................... Itziar Arrieta-Salinas, José Enrique Armendáriz-Iñigo, and Joan Navarro

An Economic Model for Maximizing Profit of a Cloud Service Provider ............................................................... Thanadech Thanakornworakij, Raja Nassar, Chokchai Box Leangsuksun, and Mihaela Paun

Security Concept and Implementation for a Cloud Based E-science Infrastructure ................................................... Thomas Ludescher, Thomas Feilhauer, and Peter Brezany

Seventh International Workshop on Frontiers in Availability, Reliability, and Security (FARES 2012)

Risk Assessment, Security Measurement, and Embedded Security

Organizational Risk Assessment Based on Attacks Repetition ...................................................................................... Marianne Azer, Ahmed Shaker, Sherif Nagy, Ahmed Raafat, and Mohamad Abuzaid

A Critical Survey of Security Indicator Approaches .................................................................................................. Manuel Rudolph and Reinhard Schwarz

Fault Tolerance and Power Consumption Analysis on Chip-Multi Processors Architectures ........................................ Hossein Khezripour and Saadat Pourmozaffari

Privacy

A Privacy preserving Approach to Call Detail Records Analysis in VoIP Systems ......................................................... Stefan Hofbauer, Kristian Beckers, and Gerald Quirchmayr
Design and Implementation of a CBR-based Privacy Agent ..........................................................317
Karin Bernsmed, Inger Anne Tøndel, and Åsmund Ahlmann Nyre

Disabilities and Authentication Methods: Usability and Security ..................................................327
Kirsi Helkala

Privacy Policy Preferences Enforced by SPARQL Query Rewriting ..................................................335
Said Oulmakhzoune, Nora Cuppens-Boulahia, Frederic Cuppens, and Stephane Morucci

Cloud Computing and Social Networks
Policy and Context Management in Dynamically Provisioned Access Control Service
for Virtualized Cloud Infrastructures ...................................................................................................343
Canh Ngo, Peter Membrey, Yuri Demchenko, and Cees de Laat

Trusted Virtual Infrastructure Bootstrapping for On Demand Services ........................................350
Peter Membrey, Keith C.C. Chan, Canh Ngo, Yuri Demchenko, and Cees de Laat

Automatic Anonymization of Natural Languages Texts Posted on Social Networking Services
and Automatic Detection of Disclosure .............................................................................................358
Hoang-Quoc Nguyen-Son, Quoc-Binh Nguyen, Minh-Triet Tran, Dinh-Thuc Nguyen,
Hiroshi Yoshiura, and Isao Echizen

First International Workshop on Security of Mobile Applications (IWSMA 2012)
E2E: An Optimized IPsec Architecture for Secure and Fast Offload .............................................365
Daniel Migault, Daniel Palomares, Emmanuel Herbert, Wei You, Gabriel Ganne, Ghada Arfaoui,
and Maryline Laurent

Location Anonymity Based on Fake Queries in Continuous Location-Based Services ..........................375
Lin Yao, Chi Lin, Guangya Liu, Fangyu Deng, and Guowei Wu

Janitor, Certificate and Jury (JCJ) Trust Scheme for Wireless Ad-hoc Networks ..............................383
Mohamad M. Abuzaid and Marianne A. Azer

Repackaging Android Applications for Auditing Access to Private Data ........................................388
Pascal Berthomé, Thomas Fécherolle, Nicolas Guilloteau, and Jean-Francois Lalande

First International Workshop on Modern Cryptography and Security Engineering (MoCrySEN 2012)

Modern Cryptography
On the Weak State in GGHN-like Ciphers ..........................................................................................397
Aleksandar Kircanski and Amr M. Youssef

Security Engineering
A Scan-Based Side Channel Attack on the NTRUEncrypt Cryptosystem ........................................402
Abdel Alim Kamal and Amr M. Youssef

Symmetry in Security Protocol Cryptographic Messages—A Serious Weakness Exploitable
by Parallel Session Attacks ..................................................................................................................410
Anca Jurcut, Tom Coffey, and Reiner Dojen
Knowledge Base Development

A Common Body of Knowledge for Engineering Secure Software and Services .................................................................499
  Widura Schwittek, Holger Schmidt, Kristian Beckers, Stefan Eicker, Stephan Faßbender,
  and Maritta Heisel

Building an Incident Management Body of Knowledge ....................................................................................................507
  David A. Mundie and Robin Ruefle

Challenges of Web-Based Information Security Knowledge Sharing ................................................................................514
  Daniel Feledi and Stefan Fenz

Applications

Using Ontologies for Adaptive Information Security Training ..........................................................................................522
  Lee V. Mangold

An Ontology for Run-Time Verification of Security Certificates for SOA ........................................................................525
  Stefania D’Agostini, Valentina Di Giacomo, Claudia Pandolfo, and Domenico Presenza

IO: An Interconnected Asset Ontology in Support of Risk Management Processes ............................................................534
  Henk Birkholz, Ingo Sieverdingbeck, Karsten Sohr, and Carsten Bormann

Sixth International Workshop on Secure Software Engineering (SecSE 2012)

Threats and Approaches

Representing Threats in BPMN 2.0 ........................................................................................................................................542
  Per Håkon Meland and Erlend Andreas Gjære

Type Classification against Fault Enabled Mutant in Java Based Smart Card .................................................................551
  Jean Dubreuil, Guillaume Bouffard, Jean-Louis Lanet, and Julien Cartigny

Towards Concurrent Data Sampling Using GPU Coprocessing .......................................................................................557
  Mark M. Seeger and Stephen D. Wolthusen

Taxonomies and Comparisons

A Taxonomy of Time and State Attacks ............................................................................................................................564
  Horia V. Corcalciuc

Comparing Privacy Requirements Engineering Approaches ..........................................................................................574
  Kristian Beckers

A Comparative Study of Software Security Pattern Classifications .................................................................................582
  Aleem Khalid Alvi and Mohammad Zulkernine

Fifth International Workshop on Digital Forensics (WSDF 2012)
Theoretical Methods and Statistics for Forensics

Uncertainty Bounds for Digital Forensic Evidence and Hypotheses ................................................................. 590
Richard E. Overill and Jantje A.M. Silomon

Using Attack Graphs in Forensic Examinations .................................................................................................. 596
Changwei Liu, Anoop Singhal, and Duminda Wijesekera

A Statistical Approach for Identifying Videos of Child Pornography at Crime Scenes .................................... 604
Mateus de Castro Polastro and Pedro Monteiro da Silva Eleuterio

Applied Forensics and Data Generation

Synthetic Data Creation for Forensic Tool Testing: Improving Performance of the 3LSPG Framework ........................................................................................................................................ 613
York Yannikos, Christian Winter, and Markus Schneider

Simplifying RAM Forensics: A GUI and Extensions for the Volatility Framework ............................................ 620
Steffen Logen, Hans Höfken, and Marko Schuba

InnoDB Database Forensics: Reconstructing Data Manipulation Queries from Redo Logs ............................ 625
Peter Frühwirt, Peter Kieseberg, Sebastian Schrittwieser, Markus Huber, and Edgar Weippl

Author Index .......................................................................................................................................................... 634