



SECURWARE 2015

The Ninth International Conference on Emerging Security Information, Systems
and Technologies

August 23 - 28, 2015

Venice, Italy

SECURWARE 2015 Editors

Rainer Falk, Siemens AG - München, Germany

Carla Merkle Westphall, Federal University of Santa Catarina, Brazil

Hans-Joachim Hof, Munich University of Applied Sciences, Germany

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2015) by International Academy, Research, and Industry Association (IARIA)
Please refer to the Copyright Information page.

Printed by Curran Associates, Inc. (2015)

International Academy, Research, and Industry Association (IARIA)
412 Derby Way
Wilmington, DE 19810

Phone: (408) 893-6407
Fax: (408) 527-6351

petre@iaria.org

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2634
Email: curran@proceedings.com
Web: www.proceedings.com

TABLE OF CONTENTS

SECURWARE 1: SECURITY MANAGEMENT

Risk Assessment Quantification in Hybrid Cloud Configuration	1
<i>Shigeaki Tanimoto, Tsutomu Konosu, Motoi Iwashita</i>	
Network Security Incident Detection Based on Network Topology Patterns	7
<i>Juris Viksna, Karlis Freivalds, Mikus Grasmanis, Peteris Rucevskis, Baiba Kaskina, Varis Teivans</i>	
Traffic Management and Access Control in Space Experiment “Kontur-2”	9
<i>Vladimir Muliukha, Vladimir Zaborovsky, Alexander Ilyashenko, Alexander Silinenko</i>	
Secure Scrum: Development of Secure Software with Scrum	15
<i>Christoph Pohl, Hans-Joachim Hof</i>	

SECURWARE 2: CRYPTOGRAPHY

Enhanced Authenticated Encryption Scheme	21
<i>Jamal Abelfatah Morad Azzam</i>	
New Directions in Applying Physical Unclonable Functions	31
<i>Rainer Falk, Steffen Fries</i>	
The Random Gate Principle	37
<i>Sheagan John, Curtis Busby-Earle</i>	
A Comparison of the PM-DC-LM Mode With Other Common Operational Block Cipher Modes	44
<i>Petr Zacek, Roman Jasek, David Malanik</i>	

SECURWARE 3: METRICS

An Improved Threshold Proxy Signature Scheme	49
<i>Akanksha Gupta, Prakash D. Vyavahare, Manish Panchal</i>	
The Use of Acceptance Test-Driven Development in the Construction of Cryptographic Software	55
<i>Alexandre Melo Braga, Daniela Castilho Schwab, André Luiz Vannucci</i>	
Secret Sharing Schemes Threshold Determination	61
<i>Armino Guerra, Ricardo Felipe Custodio</i>	
Enterprise Security Metrics with the ADVISE Meta Model Formalism	65
<i>Brett Feddersen, Ken Keefe, William H. Sanders, Carol Muehrcke, Donald Parks, Andrew Crapo, Alfredo Gabaldon, Ravi Palla</i>	

SECURWARE 4: SECURITY FRAMEWORKS, ARCHITECTURES AND PROTOCOLS I

Implementation Issues in the Construction of an Application Framework for Secure SMS Messages on Android Smartphones	67
<i>Alexandre Melo Braga, Romulo Zanco Neto, André Luiz Vannucci, Ricardo Shiguemi Hiramatsu</i>	
A Review and Analysis on Heartbleed on Italian Websites, a Year Later	74
<i>Vito Santarcangelo, Fabrizio Valenti, Muhammad Imran Tariq, Claudio Fornaro</i>	
A Detection and Prevention Algorithm for Single and Cooperative Black hole Attacks in AODV MANETs	79
<i>Saeed K. Saeed, Noureldien A. Noureldien</i>	
A Brief Survey of Nonces and Nonce Usage	85
<i>Geir M. Koiem</i>	

SECURWARE 5: SECURITY FRAMEWORKS, ARCHITECTURES AND PROTOCOLS II

A Model for Conducting Security Assessment within an Organisation	92
<i>Nor Fatimah Awang, Azizah Abd Manaf</i>	

Cloud Card Compliance Checklist: An efficient tool for securing deployment Card Solutions on the Cloud	98
<i>Hassan El Alloussi, Laila Fetjah, Abdelhak Chaichaa</i>	
Ceremony Analysis Meets Verifiable Voting: Individual Verifiability in Helios	105
<i>Taciane Martimiano, Eduardo Dos Santos, Maina Olembo, Jean Everson Martina</i>	
Mobile Agent Security using Reference Monitor-based Security Framework	112
<i>Sandhya Armoogum, Nawaz Mohamudally, Nimal Nissanke</i>	

SECURWARE 6: MALWARE AND ANTI-MALWARE

An IDS for Browser Hijacking	118
<i>Diogo Monica, Carlos Ribeiro</i>	
Monitoring of Malware Communication Channels	123
<i>Radovan Holik, Roman Jašek</i>	
Organic Principles to Counter Malware in Automotive Environments	128
<i>Robert Altschaffel, Sven Kuhlmann, Jana Dittmann, Tobias Hoppe</i>	
Apate - A Linux Kernel Module for High Interaction Honeypots	133
<i>Christoph Pohl, Michael Meier, Hans-Joachim Hof</i>	

SECURWARE 7: SMART HOME SECURITY

Automatic Human Tracking using Localization of Neighbor Node Calculation	139
<i>Tappei Yotsumoto, Kozo Tanigawa, Miki Tsuji</i>	
Implementation of a Generic ICT Risk Model using Graph Databases	146
<i>Stefan Schiebeck, Martin Latzenhofer, Brigitte Palensky, Stefan Schauer, Gerald Quirchmayr, Thomas Benesch, Johannes Göllner, Christian Meurers, Ingo Mayr</i>	
Reduction of Neighbor Node Calculations for Automatic Human Tracking System	154
<i>Miki Tsuji, Tappei Yotsumoto, Kenichi Takahashi</i>	

SECURWARE 8: INFORMATION SECURITY

Overview on Security Approaches in Intelligent Transportation Systems: Searching for Hybrid Trust Establishment Solutions for VANETs	160
<i>Christoph Ponikwar, Hans-Joachim Hof</i>	
A Novel Financial Instrument to Incentivize Investments in Information Security Controls and Mitigate Residual Risk	166
<i>Pankaj Pandey, Steven De Haes</i>	
You Are Who You Know: Leveraging Webs-of-trust for Authentication in Identity Federations	176
<i>Bob Hulsebosch, Arnout Van Velzen, Maarten Wegdam, Martijn Oostdijk, Remco Poortinga-Van Wijnen, Joost Van Dijk</i>	
Different Approaches to Security Incidents and Proposal of Severity Assessment of Security Incident	185
<i>Lukas Kralik, Roman Senkerik, Petr Stipek</i>	
Author Index	