

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Alfredo Cuzzocrea Christian Kittl  
Dimitris E. Simos Edgar Weippl Lida Xu (Eds.)

# Security Engineering and Intelligence Informatics

CD-ARES 2013 Workshops: MoCrySEn and SeCIHD  
Regensburg, Germany, September 2-6, 2013  
Proceedings



Springer

## Volume Editors

Alfredo Cuzzocrea  
ICAR-CNR  
and University of Calabria  
Rende Cosenza, Italy  
E-mail: cuzzocrea@si.deis.unical.it

Christian Kittl  
Evolaris Next Level  
Graz, Austria  
E-mail: christian.kittl@evolaris.net

Dimitris E. Simos  
SBA Research  
Vienna, Austria  
E-mail: dsimos@sba-research.org

Edgar Weippl  
Vienna University of Technology  
and SBA Research  
Vienna, Austria  
E-mail: edgar.weippl@tuwien.ac.at

Lida Xu  
Old Dominion University  
Norfolk, VA, USA  
E-mail: lxu@odu.edu

ISSN 0302-9743  
ISBN 978-3-642-40587-7  
DOI 10.1007/978-3-642-40588-4  
Springer Heidelberg New York Dordrecht London

e-ISSN 1611-3349  
e-ISBN 978-3-642-40588-4

Library of Congress Control Number: 2013946088

CR Subject Classification (1998): C.2, H.2-4, I.2, K.4.4, K.6.5, D.4.6

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

© IFIP International Federation for Information Processing 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

The Cross-Domain Conference and Workshop CD-ARES is focused on the holistic and scientific view of applications in the domain of information systems.

The idea of organizing cross-domain scientific events originated from a concept presented by the IFIP President Leon Strous at the IFIP 2010 World Computer Congress in Brisbane, which was seconded by many IFIP delegates in further discussions. Therefore CD-ARES concentrates on the many aspects of information systems in bridging the gap between the research results in computer science and the many application fields.

This effort leads us to the consideration of the various important issues of massive information sharing and data integration, which will (in our opinion) dominate scientific work and discussions in the area of information systems in the second decade of this century.

The organizers of this event who are engaged within IFIP in the area of Enterprise Information Systems (WG 8.9), Business Information Systems (WG 8.4) and Information Technology Applications (TC 5) very much welcome the typical cross-domain aspect of this event.

The collocation with the SeCIHD 2013 Workshop was another possibility to discuss the most essential application factors. Special thanks to Professor Ilsun You for all his efforts in this special track, which was held this year for the third time.

Also, we are proud to announce the Special Session Human-Computer Interaction and Knowledge Discovery (HCI-KDD), which is organized in the context of CD-ARES 2013. The ultimate goal of the task force HCI-KDD is to combine the best of two worlds: human-computer interaction (HCI), with emphasis on human intelligence, and knowledge discovery from data (KDD), dealing with computational intelligence. The cross-domain integration and appraisal of different fields provide an atmosphere in which to foster different perspectives and opinions. Special thanks to Dr. Andreas Holzinger, who made it possible to bring together researchers from diverse areas in a highly inter-disciplinary manner, to stimulate fresh ideas and encourage multi-disciplinary work.

Today, e-business depends heavily on the major cryptographic breakthroughs of almost 40 years ago. Without asymmetric cryptography, hardly any form of business transaction would be as easy to secure as it is today. We are thus very happy to have an excellent section on applied cryptography in this book.

The special track on modern cryptography and security engineering (MoCry-SEn) attracted 30 submissions of which the Program Committee selected 16 for publication in the workshop proceedings. The accepted papers dealt with symmetric-key cryptography, public-key cryptography, algorithmic cryptanalysis, software and hardware implementation of cryptographic algorithms, database

encryption and interaction between cryptographic theory and implementation issues.

The papers presented at this conference were selected after extensive reviews by the Program Committee with the essential help of associated reviewers.

We would like to thank all the Program Committee members and the reviewers who made great effort contributing their time, knowledge, and expertise and foremost the authors for their contributions.

September 2013

Alfredo Cuzzocrea  
Christian Kittl  
Dimitris E. Simos  
Edgar Weippl  
Lida Xu

# Organization

## Second International Workshop on Modern Cryptography and Security Engineering (MoCrySEn 2013)

### Program Chair

Dimitris E. Simos                      SBA Research, Austria

### Program Co-chairs

Nicolas Sendrier                      INRIA, France  
Edgar Weippl                          SBA Research, Austria

### Program Committee

Athanasios Angelakis	Leiden University, The Netherlands, Universite Bordeaux 1, France
Paulo Barreto	Universidade de Sao Paulo, Brazil
Christina Boura	Technical University of Denmark, Denmark
Pierre-Louis Cayrel	Université Jean Monnet, France
Matthieu Finiasz	CryptoExperts, France
Stefan Heyse	Ruhr-Universität Bochum, Germany
Aleksandar Hudic	SBA Research, Austria
Peter Kieseberg	SBA Research, Austria
Christos Koukouvinos	National Technical University of Athens, Greece
Spyros Magliveras	Florida Atlantic University, USA
Ayoub Otmani	University of Rouen, France
Christiane Peters	Technical University of Denmark, Denmark
Ludovic Perret	Université Pierre et Marie Curie 06 / INRIA, France
Maria Naya-Plasencia	INRIA, France
Jean-Pierre Tillich	INRIA, France
Zlatko Varbanov	Veliko Tarnovo University, Bulgaria
Amr Youssef	Concordia Institute for Information System Engineering, Canada

### External Reviewers

Adrian Dabrowski                      SBA Research, Austria  
Gregory Landais                      INRIA, France

## VIII Organization

Georg Merzdovnik	SBA Research, Austria
Rafael Misoczki	INRIA, France
Maciej Piec	SBA Research, Austria
Sebastian Schrittwieser	SBA Research, Austria

## Third International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013)

### General Chairs

Ilsun You	Korean Bible University, Republic of Korea
Fang-Yie Leu	Tunghai University, Taiwan

### General Vice-Chairs

Francesco Palmieri	Second University of Naples, Italy
Ugo Fiore	University of Naples “Federico II”, Italy

### Program Co-chairs

Aniello Castiglione	University of Salerno, Italy
Marek Ogiela	AGH University of Science and Technology, Poland

### Program Committee

Giovanni Acampora	TU/e, Eindhoven University of Technology, The Netherlands
Christina Alcaraz	University of Malaga, Spain
Joonsang Baek	Khalifa University of Science, Technology & Research, UAE
Francesca Bosco	United Nations Interregional Crime and Justice Research Institute, Italy
Antonio Colella	Italian Army, Italy
Gabriele Costa	University of Genoa, Italy
Christian Czossek	Estonian Business School, Estonia
Bonaventura D’Alessio	Carabinieri Specialist Mobile Unit Command, Italy
Massimo Ficco	Second University of Naples, Italy
Alessandro Gigante	European Space Agency, ESRIN Health, Safety and Security Officer, Italy
Tomasz Hachaj	Pedagogical University in Krakow, Poland
Leonardo Impagliazzo	Engineering Signalling Busines Unit, AnsaldoSTS, Italy

Shinsaku Kiyomoto	KDDI R&D Laboratories Inc., Japan
Giovanni Motta	Google Inc., USA
Jordi Nin	Universitat Politècnica de Catalunya, Barcelona, Spain
Kyung-Hyune Rhee	Pukyong National University, Republic of Korea
Sergio Ricciardi	Universitat Politècnica de Catalunya, Barcelona, Spain
Alessandra Sala	Bell Labs, Ireland
Germán Santos-Boada	Universitat Politècnica de Catalunya, Barcelona, Spain
Athanasios V. Vasilakos	University of Western Macedonia, Greece
Shuichiro Yamamoto	Nagoya University, Japan
Toshihiro Yamauchi	Okayama University, Japan
Siu Ming Yiu	The University of Hong Kong, SAR China
Wei Yu	Towson University, USA



# Table of Contents

## 2<sup>nd</sup> International Workshop on Modern Cryptography and Security Engineering (MoCrySEn 2013)

### *Modern Cryptography*

#### Symmetric-Key Cryptography

Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock . . . . .	1
<i>Jiageng Chen and Atsuko Miyaji</i>	
Information-Theoretically Secure Aggregate Authentication Code: Model, Bounds, and Constructions . . . . .	16
<i>Asato Kubai, Junji Shikata, and Yohei Watanabe</i>	
On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography . . . . .	29
<i>Kishan Chand Gupta and Indranil Ghosh Ray</i>	

#### Public-Key Cryptography

Code-Based Public-Key Encryption Resistant to Key Leakage . . . . .	44
<i>Edoardo Persichetti</i>	
Packed Homomorphic Encryption Based on Ideal Lattices and Its Application to Biometrics . . . . .	55
<i>Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, and Takeshi Koshiba</i>	

#### Algorithmic Cryptanalysis

A Comparison between Two Off-the-Shelf Algebraic Tools for Extraction of Cryptographic Keys from Corrupted Memory Images . . . . .	75
<i>Abdel Alim Kamal, Roger Zahno, and Amr M. Youssef</i>	
Cryptanalysis of 2-Layer Nonlinear Piece in Hand Method . . . . .	91
<i>Xuyun Nie, Albrecht Petzoldt, and Johannes Buchmann</i>	
On the Security of LBlock against the Cube Attack and Side Channel Cube Attack . . . . .	105
<i>Saad Islam, Mehreen Afzal, and Adnan Rashdi</i>	

## *Security Engineering*

### **Software and Hardware Implementation of Cryptographic Algorithms**

Code-Based Identification and Signature Schemes in Software . . . . .	122
<i>Sidi Mohamed El Yousfi Alaoui, Pierre-Louis Cayrel, Rachid El Bansarkhani, and Gerhard Hoffmann</i>	
Fast Software Polynomial Multiplication on ARM Processors Using the NEON Engine . . . . .	137
<i>Danilo Câmara, Conrado P.L. Gouvêa, Julio López, and Ricardo Dahab</i>	
Improving the Efficiency of Elliptic Curve Scalar Multiplication Using Binary Huff Curves . . . . .	155
<i>Gerwin Gsenger and Christian Hanser</i>	
Speeding Up the Fixed-Base Comb Method for Faster Scalar Multiplication on Koblitz Curves . . . . .	168
<i>Christian Hanser and Christian Wagner</i>	

### **Database Encryption**

Cumulus4j: A Provably Secure Database Abstraction Layer . . . . .	180
<i>Matthias Huber, Matthias Gabel, Marco Schulze, and Alexander Bieber</i>	

### **Interaction between Cryptographic Theory and Implementation Issues**

Optimal Parameters for XMSS <sup>MT</sup> . . . . .	194
<i>Andreas Hülsing, Lea Rausch, and Johannes Buchmann</i>	
Solving the Discrete Logarithm Problem for Packing Candidate Preferences . . . . .	209
<i>James Heather, Chris Culnane, Steve Schneider, Sriramkrishnan Srinivasan, and Zhe Xia</i>	
SPA on MIST Exponentiation Algorithm with Multiple Computational Sequences . . . . .	222
<i>Chien-Ning Chen, Jheng-Hong Tu, and Sung-Ming Yen</i>	

### 3<sup>rd</sup> International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013)

#### Cyber Security and Dependability

Cyber Threats Monitoring: Experimental Analysis of Malware Behavior in Cyberspace . . . . .	236
<i>Clara Maria Colombini, Antonio Colella, Marco Mattiucci, and Aniello Castiglione</i>	
Analyzing the Internet Stability in Presence of Disasters . . . . .	253
<i>Francesco Palmieri, Ugo Fiore, Aniello Castiglione, Fang-Yie Leu, and Alfredo De Santis</i>	
Dependency Analysis for Critical Infrastructure Security Modelling: A Case Study within the Grid'5000 Project . . . . .	269
<i>Thomas Schaberreiter, Sébastien Varrette, Pascal Bouvry, Juha Röning, and Djamel Khadraoui</i>	
How to Estimate a Technical VaR Using Conditional Probability, Attack Trees and a Crime Function . . . . .	288
<i>Wolfgang Boehmer</i>	
Using Probabilistic Analysis for the Certification of Machine Control Systems . . . . .	305
<i>Atif Mashkoor, Osman Hasan, and Wolfgang Beer</i>	
Experimental Investigation in the Impact on Security of the Release Order of Defensive Algorithms . . . . .	321
<i>Suliman A. Alsuhibany, Ahmad Alonaizi, Charles Morisset, Chris Smith, and Aad van Moorsel</i>	

#### Network Security and Privacy

A Multiple-Key Management Scheme in Wireless Sensor Networks . . . . .	337
<i>Jung-Chun Liu, Yi-Li Huang, Fang-Yie Leu, Ilsun You, Feng-Ching Chiang, Chao-Tung Yang, and William Cheng-Chung Chu</i>	
VisSecAnalyzer: A Visual Analytics Tool for Network Security Assessment . . . . .	345
<i>Igor Kotenko and Evgenia Novikova</i>	
A Denial of Service Attack to GSM Networks via Attach Procedure . . . . .	361
<i>Nicola Gobbo, Alessio Merlo, and Mauro Migliardi</i>	

PPM: Privacy Policy Manager for Personalized Services . . . . .	377
<i>Shinsaku Kiyomoto, Toru Nakamura, Haruo Takasaki, Ryu Watanabe, and Yutaka Miyake</i>	
An Attribute Based Private Data Sharing Scheme for People-Centric Sensing Networks . . . . .	393
<i>Bo Liu, Baokang Zhao, Bo Liu, and Chunqing Wu</i>	
 <b>Multimedia Technology for Homeland Defense</b>	
Intelligent UBMS Systems for Strategic Information Management . . . . .	408
<i>Lidia Ogiela and Marek R. Ogiela</i>	
Fully Distributed Secure Video Surveillance Via Portable Device with User Awareness . . . . .	414
<i>Arcangelo Castiglione, Ciriaco D'Ambrosio, Alfredo De Santis, and Francesco Palmieri</i>	
Computer Karate Trainer in Tasks of Personal and Homeland Security Defense . . . . .	430
<i>Tomasz Hachaj and Marek R. Ogiela</i>	
Trustworthiness Evaluation of Multi-sensor Situation Recognition in Transit Surveillance Scenarios . . . . .	442
<i>Francesco Flammini, Stefano Marrone, Nicola Mazzocca, Alfio Pappalardo, Concetta Pragliola, and Valeria Vittorini</i>	
A New Approach to Develop a Dependable Security Case by Combining Real Life Security Experiences (Lessons Learned) with D-Case Development Process . . . . .	457
<i>Vaise Patu and Shuichiro Yamamoto</i>	
 <b>Author Index . . . . .</b>	 465