Lecture Notes in Computer Science 8128

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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
e-ISSN 1611-3349
ISBN 978-3-642-40587-7
e-ISBN 978-3-642-40588-4
DOI 10.1007/978-3-642-40588-4
Springer Heidelberg New York Dordrecht London

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

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 (MoCrySEn) 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-Universitat 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

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 Czosseck	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 Politènica de Catalunya, Barcelona, Spain
Kyung-Hyune Rhee	Pukyong National University, Republic of Korea
Sergio Ricciardi	Universitat Politènica 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

2nd International Workshop on Modern Cryptography and Security Engineering (MoCrySEn 2013)

Modern Cryptography

Symmetric-Key Cryptography

Public-Key Cryptography

Algorithmic Cryptanalysis

Security Engineering

Software and Hardware Implementation of Cryptographic Algorithms

Database Encryption

Interaction between Cryptographic Theory and Implementation Issues

3rd International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013)

Cyber Security and Dependability

Network Security and Privacy

Multimedia Technology for Homeland Defense