Lecture Notes in Computer Science 7483

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

Dieter Gollmann Felix C. Freiling (Eds.)

Information Security

15th International Conference, ISC 2012
Passau, Germany, September 19-21, 2012
Proceedings

Springer

Volume Editors

Dieter Gollmann
Hamburg University of Technology, Institute for Security in Distributed Applications
Harburger Schlossstrasse 20, 21073, Hamburg, Germany
E-mail: diego@tu-harburg.de

Felix C. Freiling
Friedrich-Alexander-University, Department of Computer Science
Martenstrasse 3, 91058 Erlangen, Germany
E-mail: felix.freiling@cs.fau.de

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-33382-8 e-ISBN 978-3-642-33383-5
DOI 10.1007/978-3-642-33383-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012946460

CR Subject Classification (1998): E.3, E.4, D.4.6, K.6.5, C.2, J.1, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

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)

Foreword

Information security continues to be a topic of great relevance to society. The Information Security Conference (ISC) is an annual international conference dedicated to research on the theory and applications of information security. The 2012 conference was the 15^{th} in the conference series that started as a workshop in 1997, changed to a conference in 2001, and has been held on five different continents since. Hosted by the University of Passau in Lower Bavaria, ISC 2012 was the first conference in this series to be held in Germany.

ISC 2012 attracted high-quality papers on all technical aspects of information security. We received 72 submissions, which were reviewed by at least three members of the program committee. We finally accepted 23 papers, which are collected in these proceedings. In addition, we invited Isabel Trancoso and her colleagues to speak on privacy issues in speech processing. A second keynote speech was given by Michael Waidner from Fraunhofer SIT and Technische Universität Darmstadt.

We wish to thank all the people who invested time and energy to make ISC 2012 a success: First and foremost come all the authors who submitted papers to ISC and presented them at the conference. The members of the program committee together with all the external reviewers worked hard in evaluating the submissions and, in some cases, in shepherding promising work. The ISC steering committee, in particular Masahiro Mambo, helped us graciously in all critical decisions. Thanks also go to the 2012 general chair Joachim Posegga and his team at Passau University for handling the local arrangements, to Eric Rothstein for maintaining the conference website, and to Isaac Agudo and Cheng-Kang Chu for their efforts as publicity chairs.

July 2012

Dieter Gollmann
Felix C. Freiling

Organization

General Chair

Joachim Posegga	University of Passau, Germany

Steering Committee Chair

Masahiro Mambo	Kanazawa University, Japan

Program Chairs

Dieter Gollmann	Hamburg University of Technology, Germany
Felix C. Freiling	Friedrich-Alexander-Universität, Erlangen, Germany

Program Committee

Magnus Almgren	Chalmers University of Technology, Sweden
Tuomas Aura	Aalto University, Finland
Joonsang Baek	KUSTAR, UAE
Alex Biryukov	University of Luxembourg, Luxembourg
Sonja Buchegger	KTH Royal Institute of Technology, Sweden
Liqun Chen	HP Laboratories Bristol, UK
Xiaofeng Chen	Xidian University, P.R. China
Chen-Mou Cheng	National Taiwan University, Taiwan
Sherman S.M. Chow	University of Waterloo, Canada
Jorge Cuellar	Siemens, Germany
Vanesa Daza	Universitat Pompeu Fabra, Spain
Claudia Diaz	KU Leuven, Belgium
Roberto Di Pietro	Università degli Studi Roma Tre, Italy
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Bao Feng	Institute for Infocomm Research, Singapore
Eduardo B. Fernandez	Florida Atlantic University, USA
Josep Ferrer	University of the Balearic Islands, Spain
Sara Foresti	Università degli Studi di Milano, Italy
Stefanos Gritzalis	University of the Aegean, Greece
Thorsten Holz	Ruhr-Universität Bochum, Germany
Martin Johns	SAP, Germany
Angelos Keromytis	Columbia University, USA
Igor Kotenko	Russian Academy of Sciences, Russia
Xuejia Lai	Shanghai Jiao Tong University, P.R. China

Zhenkai Liang	National University of Singapore, Singapore
Peng Liu	Pennsylvania State University, USA
Javier López	Universidad de Málaga, Spain
Masahiro Mambo	Kanazawa University, Japan
Mark Manulis	TU Darmstadt, Germany
Atsuko Miyaji	JAIST, Japan
Jose Morales	Carnegie Mellon University, USA
Raphael C.-W. Phan	Loughborough University, UK
Frank Piessens	KU Leuven, Belgium
Christian W. Probst	Technical University of Denmark, Denmark
Vincent Rijmen	KU Leuven, Belgium
Matt Robshaw	Orange Labs, France
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Jörg Schwenk	Ruhr-Universität Bochum, Germany
Jan Seedorf	NEC Laboratories Europe, Germany
Miguel Soriano	Universitat Politècnica de Catalunya, Spain
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Kyushu University, Japan
Lingyu Wang	Concordia University, Canada
Susanne Wetzel	Stevens Institute of Technology, USA
Duncan Wong	City University of Hong Kong, P.R. China
Jeff Yan	Newcastle University, UK
S.M. Yiu	University of Hong Kong, P.R. China
Jianying Zhou	Institute for Infocomm Research, Singapore
Alf Zugenmaier	Hochschule München, Germany

Additional Reviewers

Man Ho Au	Javier Herranz
Werner Backes	Jialin Huang
Oleksandr Bodriagov	Kangkook Jee
Andrey Chechulin	Christos Kalloniatis
Kai Yuen Cheong	Ergina Kavallieratou
Tat Wing Chim	Gunnar Kreitz
Cheng-Kang Chu	Po-Chun Kuo
Willem De Groef	Sebastian Lekies
Philippe De Ryck	Gaëtan Leurent
Xinshu Dong	Wei Li
Ming Duan	Yue-Hsun Lin
Sebastian Gajek	Flavio Lombardi
Wei Gao	Nikolaos Makriyannis
Stefano Guarino	Daniel A. Mayer
Seda Gurses	Kirill Morozov

Nick Nikiforakis
Evgenia Novikova
Kazumasa Omote
Kailas Patil
Constantinos Patsakis
Alfredo Rial
Panagiotis Rizomiliotis
Santi Martinez Rodriguez
Rodrigo Roman
Arnab Roy
Igor Saenko
Bagus Santoso
Theodoor Scholte
Nicolas Sendrier
Isamu Teranishi
Elmar Tischhauser
Aggeliki Tsochou
Frederik Vercauteren
José Luis Vivas
Huaqun Wang
Baodian Wei
Ralf-Philipp Weinmann
Jia Xu
Kenji Yasunaga
Eunjung Yoon
Bin Zhao
Hang Zhao
Yuanjie Zhao
Hui Zhang
Tao Zhang
Yinghui Zhang
Chen Zhong
Youwen Zhu

Publicity Chairs

Isaac Agudo	Universidad de Málaga, Spain
Cheng-Kang Chu	National Chiao Tung University, Taiwan

Local Organization

Marita Güngerich, Siglinde Böck, Eric Rothstein

Table of Contents

Software Security

Processing Encrypted Data

Authentication and Identification

New Directions in Access Control

GPU for Security

Models for Risk and Revocation