Lecture Notes in Computer Science 6531

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

Mike Burmester
Gene Tsudik
Spyros Magliveras
Ivana Ilić (Eds.)

Information Security

13th International Conference, ISC 2010
Boca Raton, FL, USA, October 25-28, 2010
Revised Selected Papers

Springer

Volume Editors

Mike Burmester
Department of Computer Science
Florida State University
Tallahassee, FL, 32306-4530, USA
E-mail: burmester@cs.fsu.edu

Gene Tsudik
Department of Computer Science
University of California
Irvine, CA, 92697-3425, USA
E-mail: gts@ics.uci.edu

Spyros Magliveras
Department of Mathematical Sciences
Florida Atlantic University
Boca Raton, FL, 33431-0991 , USA
E-mail: spyros@fau.edu

Ivana Ilić
Department of Mathematical Sciences
Florida Atlantic University
Boca Raton, FL, 33431-0991, USA
E-mail: iva_ilic@yahoo.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-18177-1 e-ISBN 978-3-642-18178-8
DOI 10.1007/978-3-642-18178-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2010942728

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

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)

Preface

The 13^{th} Information Security Conference (ISC 2010) was held at Deerfield Beach / Boca Raton, Florida, USA, during October 25–28, 2010. The conference was hosted by the Center for Cryptology and Information Security (CCIS) at the Mathematical Sciences Department of Florida Atlantic University in Boca Raton, Florida.

ISC is an annual international conference covering research in theory and applications of information security and aims to attract high quality-papers in all technical aspects of information security as well as to provide a forum for professionals from academia and industry to present their work and exchange ideas. We are very pleased with both the number and high quality of this year's submissions. The Program Committee received 117 submissions, and accepted 25 as full papers (acceptance rate 21%). The papers were selected after an extensive and careful refereeing process in which each paper was reviewed by at least three members of the Program Committee. A further 11 articles were selected as short papers because of their appropriateness and high quality. A new experimental format was adopted this year: pre-conference proceedings of all accepted papers were made available at the conference. This provided an additional opportunity for authors to solicit and obtain early feedback. The Springer proceedings were mailed to the authors after the conference.

Many people deserve our gratitude for their generous contributions to the success of this conference. We wish to thank all the members of the ISC 2010 Program Committee, as well as the external reviewers, for reviewing, deliberating and selecting (under severe time pressure and in the middle of summer) an excellent set of papers. Thanks are also due to Masahiro Mambo who, as our contact person on the ISC Steering Committee, helped maintain ISC traditions and provided guidance. Mega-kudos to Ivana Ilić for contributing a tremendous amount of work, much of it beyond the call of duty. Also, a great deal of thanks are due to: Emily Cimillo for helping with budgetary issues, Leanne Magliveras for keeping track of numerous organizational tasks, as well as Nidhi Singhi, Nikhil Singhi and Nicola Pace for invaluable assistance with various conference aspects.

We are delighted to acknowledge the sponsorship of CCIS; of the Center for Security and Assurance in IT (C-SAIT) of Florida State University; of the Charles E. Schmidt College of Science at Florida Atlantic University; and of the DATAMAXX group, the latter having provided support for the *Best Student Paper Awards* and additional funds for graduate student support.

Last but not least, on behalf of all those involved in organizing the conference we would like to thank all the authors who submitted papers to this conference. Without their submissions and support, ISC could not have been a success.

November 2010

Spyros Magliveras
Mike Burmester
Gene Tsudik

Organization

General Chair

Spyros Magliveras	CCIS, Florida, USA

Program Committee Co-chairs

Mike Burmester	Florida State University, USA
Gene Tsudik	University of California, Irvine, USA

Program Committee

Giuseppe Ateniese	Johns Hopkins University, USA
Elisa Bertino	Purdue University, USA
Simon Blackburn	Royal Holloway, UK
Ian Blake	University of Toronto, Canada
Marina Blanton	University of Notre Dame, USA
Carlo Blundo	Università di Salerno, Italy
Colin Boyd	Queensland University of Technology Australia
Levente Buttyan	Budapest University of Technology and Economics, Hungary
Cafer Caliskan	Michigan Technical University Michigan, USA
Claude Castelluccia	INRIA, France
David Chadwick	University of Kent, UK
Jung Hee Cheon	Seoul National University, Korea
Emiliano De Cristofaro	University of California, Irvine, USA
Vanesa Daza	Universitat Pompeu Fabra, Spain
Claudia Diaz	KU Leuven, Belgium
Roberto Di Pietro	Roma Tre University, Italy
Xuhua Ding	Singapore Management University, Singapore
Wenliang Du	Syracuse University, France
Thomas Eisenbarth	CCIS, Florida, USA
Eduardo Fernandez	Florida Atlantic University, USA
Juan Garay	ATT Research, USA
Madeline Gonzalez	Cybernetica AS, Estonia
Nick Hopper	University of Minnesota, USA
Ivana Ilić	CCIS, Florida, USA

Kwangjo Kim	KAIST, Korea
Yongdae Kim	University of Minnesota, USA
Panos Kotzanikolaou	University of Piraeus, Greece
Feifei Li	Florida State University, Florida, USA
Javier Lopez	University of Malaga, Spain
Di Ma	University of Michigan, Dearborn, USA
Masahiro Mambo	University of Tsukuba, Japan
Emmanouil Magkos	University of the Ionian, Greece
Mark Manulis	TU Darmstadt, Germany
Ken Matheis	CCIS, Florida, USA
Nasir Memon	New York Polytechnic, New York, USA
Alfred Menezes	University of Waterloo, Canada
Ron Mullin	University of Waterloo, Canada
Jorge Munilla	Universidad de Málaga, Spain
David Naccache	ENS and Université Paris II, France
Juan Gonzalez Nieto	Queensland University of Technology Australia
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Nitesh Saxena	CS Dept, Polytechnic Institute of NYU USA
Elaine Shi	PARC, USA
Radu Sion	Stony Brook University, USA
Nikhil Singhi	CCIS, Florida, USA
Nidhi Singhi	CCIS, Florida, USA
Claudio Soriente	Madrid Polytechnic, Spain
Michal Sramka	Universitat Rovira i Virgili, Spain
Rainer Steinwandt	CCIS, Florida, USA
Doug Stinson	University of Waterloo, Canada
Jonathan Trostle	Johns Hopkins University, USA
Patrick Traynor	Georgia Institute of Technology, USA
Tran van Trung	University of Essen-Duisburg, Germany
Ivan Visconti	Università di Salerno, Italy
Bogdan Warinschi	University of Bristol, UK
Shouhuai Xu	University of Texas at San Antonio USA
Sencun Zhu	Pennsylvania State University, USA

External Reviewers

Gegerly Acs
Andrey Bogdanov
Sanjit Chatterjee
Mauro Conti
Elke De Mulder
Sara Foresti
Tim Gueneysu
Darrel Hankerson
Jens Hermans
Seokhie Hong
Vincenzo Iovino
Yoonchan Jhi
B. Hoon Kang
Jihye Kim
Kerstin Lemke-Rust
Gabriel Maganis
Amir Moradi
Franciso Moyano
Yuan Niu
Andrs Ortiz
Sai Teja Peddinti
Benny Pinkas
Stefan Schiffner
Gautham Sekar
Douglas Stebila
Germn Sez
Nino V. Verde
Jonathan Voris
Wei Xu
Aaram Yun
Lei Zhang
Claudio A. Ardagna
Eric Chan-Tin
Andrew Clark
Sabrina De Capitani di Vimercati
Carmen Fernandez
Aurelien Francillon
Tzipora Halevi
Kristiyan Haralambiev
Javier Herranz
Sebastiaan Indesteege
Rob Jansen
Seny Kamara
Jaeheon Kim
Taekyoung Kwon
Zi Lin
Joan Mir
Jose Morales
Arvind Narayanan
Jose A. Onieva
Abhi Pandya
Daniele Perito
Alessandra Scafuro
Max Schuchard
Jae Hong Seo
Dongdong Sun
Anthony Van Herrewege
Jose L. Vivas
Qianhong Wu
Li Xu
Zhenxin Zhan

Table of Contents

Attacks and Analysis

Analysis

Authentication, PIR and Content Identification

Privacy

Malware, Crimeware and Code Injection

Intrusion Detection

Side Channels

Cryptography

Smartphones

Biometrics

Cryptography, Application

Buffer Overflow

Cryptography, Theory