Lecture Notes in Computer Science 7807

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

Editorial Board

More information about this series at http://www.springer.com/series/7410

Yvo Desmedt (Ed.)

Information Security

16th International Conference, ISC 2013
Dallas, Texas, November 13–15, 2013
Proceedings

Springer

Editor
Yvo Desmedt
The University of Texas at Dallas
Richardson, TX
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-27658-8 ISBN 978-3-319-27659-5 (eBook)
DOI 10.1007/978-3-319-27659-5

Library of Congress Control Number: 2015957049

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by SpringerNature
The registered company is Springer International Publishing AG Switzerland

Preface

The Information Security Conference (ISC), which started as a workshop (ISW) in 1997, is an international conference organized yearly. It has been held in five different continents.

ISC 2013 was organized in cooperation with the International Association for Cryptologic Research, and the Department of Computer Science, The University of Texas at Dallas, USA.

There were 70 submitted papers, which were considered by the Program Committee. This is roughly the same as for ISC 2012, which took place in Passau, Germany, and had 72 submissions. Owing to the large number of submissions, some papers that contained new ideas had to be rejected. Priority was given to novel papers. Of the 70 submissions, 16 were selected, which is a 23 % acceptance rate. We also accepted 14 short papers. Each paper was sent to at least three members of the Program Committee for comments. Submissions to ISC 2013 were required to be anonymous. EasyChair was used for submissions, refereeing, etc.

Beside the accepted papers, two invited presentations were given. Michael Reiter (University of North Carolina at Chapel Hill) spoke about "How to Misuse, Use, and Mitigate Side Channels in Virtualized Environments." G.R. Blakley (IACR Fellow) spoke about his joint work with Bob Blakley and Sean Blakley on "How to Draw Graphs: Seeing and Redrafting Large Networks in Security and Biology."

The proceedings contain all the regular papers and short papers accepted, except for the paper "Formal Analysis of ECC-Based Direct Anonymous Attestation Schemes in Applied Pi Calculus," by Li Xi, Yu Qin, and Dengguo Feng. Revisions of papers were not checked for correctness on their scientific aspects and the authors bear full responsibility for the content of their papers. Some of the papers may have been edited taking the comments of the Program Committee or external referees into account.

I am very grateful to the members of the Program Committee for their hard work and the difficult task of selecting the papers. The Program Committee appreciates the effort of the external referees who helped the Program Committee reach their decisions.

I thank the general chair, Bhavani Thuraisingham, and the local chair, Kevin Hamlen, for their help in organizing ISC 2013, and Stacy Morrison for some of the local organization aspects. Moreover, Julie Weekly helped with secretarial work and Jeyakesavan Veerasamy with the registration process.

Finally, I would like to thank everyone who submitted their work to ISC 2013.

September 2015 Yvo Desmedt

ISC 2013

The 15th Information Security Conference was held in in cooperation with the International Association for Cryptologic Research, and the Department of Computer Science, The University of Texas at Dallas.

General Chair

Bhavani Thuraisingham	The University of Texas at Dallas, USA

Local Chair

Kevin Hamlen	The University of Texas at Dallas, USA

Steering Committee Chair

Masahiro Mambo	Kanazawa University, Japan

Program Chair

Yvo Desmedt	The University of Texas at Dallas, USA; and University College London, UK

Local Organizing Committee

Yvo Desmedt
Kevin Hamlen
Stacy Morrison
Bhavani Thuraisingham

Program Committee

Alessandro Acquisti	Carnegie Mellon University, USA
Elisa Bertino	Purdue University, USA
Jean Camp	Indiana University, USA
K.P. Chow	University of Hong Kong, SAR China
Ed Dawson	QUT, Australia
Sabrina De Capitani Di Vimercati	University of Milan, Italy
Yvo Desmedt (Chair)	The University of Texas at Dallas, USA; and University College London, UK
Manuel Egele	Carnegie Mellon University, USA

Hanaoka Goichiro	AIST, Japan
Thomas Gross	University of Newcastle, UK
Yong Guan	Iowa State University, USA
Sushil Jajodia	George Mason University, USA
Audun Jøsang	University of Oslo, Norway
Guenter Karjoth	IBM Zurich, Switzerland
Brian King	Indiana University-Purdue University, Indianapolis, USA
Silvio Lattanzi	Google, USA
Benoit Libert	Technicolor, France
Helger Lipmaa	University of Tartu, Estonia
Javier Lopez	University of Malaga, Spain
Stephen Mclaughlin	Pennsylvania State University, USA
Atsuko Miyaji	JAIST, Japan
David Naccache	University of Paris II, France
Tatsuaki Okamoto	NTT Labs, Japan
Giuseppe Persiano	University of Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
Bart Preneel	Catholic University of Leuven, Belgium
Rei Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	University of Milan, Italy
Joshua Schiffman	AMD, USA
Gene Spafford	Purdue University, USA
John Steinberger	Tsinghua University, China
Ron Steinfeld	Monash University Australia
Tsuyoshi Takagi	Kyushu University, Japan
Catherine Tucker	MIT, USA
Vijay Varadharajan	Macquarie University, Australia
Meiqin Wang	Shandong University, China
Yongge Wang	University of North Carolina Charlotte, USA
Danfeng Yao	Virginia Tech, USA
John Zic	CSIRO, Australia

Additional Reviewers

Albanese, Massimiliano
Alcaraz, Cristina
Alimomeni, Mohsen
Balasch, Josep
Bilgin, Begül
Camp, Jean
Chen, Jiageng
Cheng, Shu
Devigne, Julien
Fong, Philip
Futa, Yuichi
Gierlichs, Benedikt
Gupta, Aditi
Hayashi, Takuya
Hori, Yoshiaki
Jiang, Shaoquan
Kawai, Yutaka
Kobayashi, Tetsutaro
Liu, Zhenhua
Livraga, Giovanni
Min, Byungho
Morozov, Kirill
Ohata, Satsuya
Persichetti, Edoardo
Sakai, Yusuke
Sendrier, Nicolas
Shebaro, Bilal
Shin, Seonghan
Shirase, Masaaki
Sirvent, Thomas
Su, Chunhua
Sun, Kun
Tibouchi, Mehdi
Tupakula, Uday
Van Herrewege, Anthony
Varici, Kerem
Wang, Haining
Wang, Pengwei
Wei, Puwen
Xeng, Xifan
Yanai, Naoto
Yiu, Siu Ming
Yoneyama, Kazuki
Yoshino, Masayuki
Zhang, Hui
Zhang, Tongjie
Zhao, Fangming
Zhou, Lan

Contents

Usability and Risk Perception

Access Control

Computer Security

Privacy Attacks

Cryptography