Lecture Notes in Computer Science **9326**

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

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

Günther Pernul · Peter Y A Ryan
Edgar Weippl (Eds.)

Computer Security – ESORICS 2015

20th European Symposium on Research in Computer Security
Vienna, Austria, September 21–25, 2015
Proceedings, Part I

Springer

Editors
Günther Pernul
University of Regensburg
Regensburg
Germany

Peter Y A Ryan
University of Luxembourg
Luxembourg
Luxembourg

Edgar Weippl
SBA Research
Wien
Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-24173-9 ISBN 978-3-319-24174-6 (eBook)
DOI 10.1007/978-3-319-24174-6

Library of Congress Control Number: 2015948157

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Foreword

It is our great pleasure to welcome you to the 20th European Symposium on Research in Computer Security (ESORICS 2015).

This year's symposium continues its tradition of establishing a European forum for bringing together researchers in the area of computer security, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

The call for papers attracted 293 submissions – a record in the ESORICS series – from 41 countries. The papers went through a careful review process and were evaluated on the basis of their significance, novelty, technical quality, as well as on their practical impact and/or their level of advancement of the field's foundations. Each paper received at least three independent reviews, followed by extensive discussion. We finally selected 59 papers for the final program, resulting in an acceptance rate of 20 %.

The program was completed with keynote speeches by Sushil Jajodia, George Mason University Fairfax, USA and Richard Clayton, University of Cambridge, UK.

Putting together ESORICS 2015 was a team effort. We first thank the authors for providing the content of the program. We are grateful to the Program Committee, who worked very hard in reviewing papers (more than 880 reviews were written) and providing feedback for authors. There is a long list of people who volunteered their time and energy to put together and organize the conference, and who deserve special thanks: the ESORICS Steering Committee, and its chair Pierangela Samarati in particular, for their support; Giovanni Livraga, for taking care of publicity; Javier Lopez, as workshop chair, and all workshop co-chairs, who organized workshops co-located with ESORICS; and Yvonne Poul for the local organization and the social events.

Finally, we would like to thank our sponsors, HUAWEI, for the financial support and SBA Research, for hosting and organizing ESORICS 2015.

A different country hosts the conference every year. ESORICS 2015 took place in Vienna, Austria at the Vienna University of Technology. We are very happy to have hosted the 20th edition of the symposium in Vienna and we tried to put together a special social program for you, giving you the opportunity to share ideas with other researchers and practitioners from institutions around the world and see all the beautiful sights of Vienna.

We hope that you found this program interesting and thought-provoking and that you enjoyed ESORICS 2015 and Vienna.

July 2015

Günther Pernul
Peter Y A Ryan
Edgar Weippl

Organization

General Chair

Günther Pernul	Universität Regensburg, Germany

Program Chairs

Peter Y A Ryan	University of Luxembourg, Luxembourg
Edgar Weippl	SBA Research & Vienna University of Technology, Austria

Workshops Chair

Javier Lopez	University of Malaga, Spain

Program Committee

Alessandro Armando	Università di Genova, Italy
Vijay Atluri	Rutgers University, USA
Michael Backes	Saarland University, Germany
Feng Bao	Security and Privacy Lab, Huawei, China
David A. Basin	ETH Zurich, Switzerland
Giampaolo Bella	Università di Catania, Italy
Carlo Blundo	Università degli Studi di Salerno, Italy
Stefan Brunthaler	SBA Research, Austria
Ran Canetti	Tel Aviv University, Israel
Liqun Chen	HP Labs, UK
Michael Clarkson	Cornell University, USA
Jason Crampton	University of London, UK
Cas Cremers	University of Oxford, UK
Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Boulahia	Télécom Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Wenliang Du	Syracuse University, USA
Hannes Federrath	University of Hamburg, Germany
Simon Foley	University College Cork, Ireland
Sara Foresti	Università degli Studi di Milano, Italy
Felix Freiling	Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Michael Goldsmith	University of Oxford, UK

Dieter Gollmann	TU Hamburg-Harburg, Germany
Dimitris Gritzalis	AUEB, Greece
Joshua Guttman	MTIRE Corp and Worcester Polytechnic, USA
Feng Hao	Newcastle University, UK
Amir Herzberg	Bar-Ilan University, Israel
Xinyi Huang	Fujian Normal University, China
Michael Huth	Imperial College, UK
Sotiris Ioannidis	FORTH, Crete
Sushil Jajodia	George Mason University, USA
Markus Jakobsson	Qualcomm, USA
Sokratis K. Katsikas	University of Piraeus, Greece
Stefan Katzenbeisser	TU Darmstadt, Germany
Florian Kerschbaum	SAP, Germany
Steve Kremer	INRIA Nancy and LORIA, France
Adam J. Lee	University of Pittsburgh, USA
Wenke Lee	Georgia Institute of Technology, USA
Yingjiu Li	Singapore Management University, Singapore
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Wenjing Lou	Virginia Polytechnic Institute and State University, USA
Haibing Lu	Santa Clara University, USA
Antonio Maña	Univeristy of Malaga, Spain
Roy Maxion	Carnegie Mellon University, USA
Catherine Meadows	Naval Research Laboratory, USA
Carroll Morgan	University of New South Wales, Australia
John C. Mitchell	Stanford University, USA
Martin Mulazzani	SBA Research, Austria
David Naccache	ENS, France
Rolf Oppliger	eSecurity Technologies, Switzerland
Stefano Paraboschi	Università degli Studi di Bergamo, Italy
Olivier Pereira	UCL Crypto Group, Belgium
Günther Pernul	University of Regensburg, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater	UCL, Belgium
Kui Ren	University at Buffalo, State University of New York, USA
Mark Ryan	University of Birmingham, UK
Ahmad-Reza Sadeghi	TU Darmstadt, Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Nitesh Saxena	University of Alabama at Birmingham, USA
Andreas Schaad	SAP, Germany
Steve Schneider	University of Surrey, UK
Jörg Schwenk	Ruhr University Bochum, Germany
Basit Shafiq	Lahore University of Management Sciences, Pakistan
Dimitris E. Simos	SBA Research, Austria

Einar Snekkenes	Gjovik University College, Norway
Philip Stark	University of California, Berkeley, USA
Vanessa Teague	University of Melbourne, Australia
Jaideep Vaidya	Rutgers University, USA
Paulo Verissimo	University of Luxembourg, Luxembourg
Luca Viganò	King's College London, UK
Michael Waidner	TU Darmstadt, Germany
Cong Wang	City University of Hong Kong, China
Lingyu Wang	University of Concordia, Canada
Ting Yu	North Carolina State University, USA
Meng Yu	Virginia Commonwealth University, USA
Moti Yung	Google, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Sencun Zhu	Pennsylvania State University, USA

Contents – Part I

Contents – Part II

Protocols and Attribute-Based Encryption

Code Analysis and Side-Channels

Detection and Monitoring

Authentication

Policies

Applied Security