IFIP Advances in Information and Communication Technology 502

Editor-in-Chief

Kai Rannenberg, Goethe University Frankfurt, Germany

Editorial Board

TC 1 – Foundations of Computer Science
Jacques Sakarovitch, Télécom ParisTech, France

TC 2 – Software: Theory and Practice
Michael Goedicke, University of Duisburg-Essen, Germany

TC 3 – Education
Arthur Tatnall, Victoria University, Melbourne, Australia

TC 5 – Information Technology Applications
Erich J. Neuhold, University of Vienna, Austria

TC 6 – Communication Systems
Aiko Pras, University of Twente, Enschede, The Netherlands

TC 7 – System Modeling and Optimization
Fredi Tröltzsch, TU Berlin, Germany

TC 8 – Information Systems
Jan Pries-Heje, Roskilde University, Denmark

TC 9 – ICT and Society
Diane Whitehouse, The Castlegate Consultancy, Malton, UK

TC 10 – Computer Systems Technology
Ricardo Reis, Federal University of Rio Grande do Sul, Porto Alegre, Brazil

TC 11 – Security and Privacy Protection in Information Processing Systems
Steven Furnell, Plymouth University, UK

TC 12 – Artificial Intelligence
Ulrich Furbach, University of Koblenz-Landau, Germany

TC 13 – Human-Computer Interaction
Marco Winckler, University Paul Sabatier, Toulouse, France

TC 14 – Entertainment Computing
Matthias Rauterberg, Eindhoven University of Technology, The Netherlands

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the first World Computer Congress held in Paris the previous year. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

> *IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.*

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is generally smaller and occasionally by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

More information about this series at http://www.springer.com/series/6102

Sabrina De Capitani di Vimercati
Fabio Martinelli (Eds.)

ICT Systems Security and Privacy Protection

32nd IFIP TC 11 International Conference, SEC 2017
Rome, Italy, May 29–31, 2017
Proceedings

Springer

Editors
Sabrina De Capitani di Vimercati
Università degli Studi di Milano
Crema
Italy

Fabio Martinelli
National Research Council of Italy
Pisa
Italy

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-58468-3 ISBN 978-3-319-58469-0 (eBook)
DOI 10.1007/978-3-319-58469-0

Library of Congress Control Number: 2017939343

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers selected for presentation at the 32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2017), held in Rome, Italy, May 29–31, 2017. IFIP SEC conferences are the flagship events of the International Federation for Information Processing (IFIP) Technical Committee 11 on Information Security and Privacy Protection in Information Processing Systems (TC-11).

In response to the call for papers, 199 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was assigned to at least four members of the Program Committee. The Program Committee meeting was held electronically, with intensive discussion over a period of two weeks. Of the papers submitted, 38 were selected for presentation at the conference.

A conference like this does not just happen; it depends on the volunteer efforts of a host of individuals. There is a long list of people who volunteered their time and energy to put together the conference and who deserve acknowledgment. Thanks to all the members of the Program Committee, and the external reviewers, for all their hard work in the paper evaluation. We are very grateful to everyone who gave their assistance and ensured a smooth organization process: Sara Foresti, Luigi V. Mancini (General Chairs); Giovanni Livraga (Publicity Chair); Adriana Lazzaroni (Local Organizing Chair); Patrizia Andronico, Raffaella Casarosa, and Giulia Severino (Local Organizing Secretariat). A special thanks goes to the keynote speakers who accepted our invitation to deliver keynote talks at the conference. We are also sincerely grateful to our sponsor, NECS.

Last but certainly not least, thanks to all the authors who submitted papers and all the conference's attendees. We hope you find the proceedings of IFIP SEC 2017 interesting, stimulating, and inspiring for your future research.

May 2017

Sabrina De Capitani di Vimercati
Fabio Martinelli

Organization

General Chairs

Sara Foresti	Università degli Studi di Milano, Italy
Luigi V. Mancini	University of Roma La Sapienza, Italy

Program Chairs

Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Fabio Martinelli	National Research Council of Italy, Italy

Publicity Chair

Giovanni Livraga	Università degli Studi di Milano, Italy

Local Organizing Chair

Adriana Lazzaroni	National Research Council of Italy, Italy

Local Organizing Secretariat

Patrizia Andronico	National Research Council of Italy, Italy
Raffaella Casarosa	National Research Council of Italy, Italy
Giulia Severino	National Research Council of Italy, Italy

Program Committee

Soon Aechun	City University of New York, USA
Vijay Atluri	Rutgers University, USA
Maurizio Aiello	National Research Council of Italy, Italy
Roberto Baldoni	University of Rome La Sapienza, Italy
Matt Bishop	University of California, Davis, USA
Rainer Boehme	University of Innsbruck, Austria
Andrea Bondavalli	Università degli Studi di Firenze, Italy
Joppe Bos	NXP Semiconductors, Belgium
Yazan Boshmaf	Qatar Computing Research Institute, Qatar
Dagmar Brechlerová	Euromise, Czech Republic
William Caelli	IISEC Pty Ltd., Australia
Jan Camenisch	IBM Research Zurich, Switzerland
Iliano Cervesato	Carnegie Mellon University, Qatar
Nathan Clarke	University of Plymouth, UK

Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Boulahia	Télécom Bretagne, France
Christian Damsgaard Jensen	Technical University of Denmark, Denmark
Bart De Decker	KU Leuven, Belgium
Gurpreet Dhillon	Virginia Commonwealth University, USA
Tassos Dimitrou	Greece and Kuwait University, Kuwait
Roberto Di Pietro	Nokia Bell Labs, France
Carmen Fernandez-Gago	University of Malaga, Spain
Simone Fischer-Hübner	Karlstad University, Sweden
William Fitzgerald	Johnson Controls, Ireland
Sara Foresti	Università degli Studi di Milano, Italy
Lynn Futcher	NMMU, South Africa
Steven Furnell	University of Plymouth, UK
Joaquin Garcia-Alfaro	Telecom SudParis, France
Dieter Gollmann	Hamburg University of Technology, Hamburg
Stefanos Gritzalis	University of the Aegean, Greece
Sushil Jajodia	George Mason University, USA
Lech Janczewski	The University of Auckland, New Zealand
Martin Johns	SAP Research, Germany
Wouter Joosen	Katholieke Universiteit Leuven, Belgium
Audun Josang	University of Oslo, Norway
Sokratis Katsikas	NTNU, Norway
Kwangjo Kim	KAIST, Republic of Korea
Florian Kerschbaum	University of Waterloo, Canada
Dogan Kesdogan	Universität Regensburg, Germany
Igor Kotenko	SPIIRAS, Russia
Zbigniew Kotulski	Warsaw University of Technology, Poland
Peter Lambert	DST Group, Australia
Gert Læssøe Mikkelsen	The Alexandra Institute, Denmark
Adam J. Lee	University of Pittsburgh, USA
Giovanni Livraga	Università degli Studi di Milano, Italy
Javier Lopez	University of Malaga, Spain
Evangelos Markatos	ICS/FORTH, Greece
Stephen Marsh	UOIT, Canada
Refik Molva	EURECOM, France
Paolo Mori	National Research Council of Italy, Italy
Yuko Murayama	Iwate Prefectural University, Japan
Eiji Okamoto	University of Tsukuba, Japan
Daniel Olejar	Comenius University, Slovakia
Panos Papadimitratos	KTH, Sweden
András Pataricza	BME, Hungary
Philippos Peleties	CCS, Cyprus
Günther Pernul	Universität Regensburg, Germany
Giuseppe Persiano	Università degli Studi di Salerno, Italy
Gilbert Peterson	AFIT, USA

Wolter Pieters	TU Delft, The Netherlands
Joachim Posegga	University of Passau, Germany
Alexander Pretschner	Technical University of Munich, Germany
Sihan Qing	Peking University, China
Kai Rannenberg	Goethe University Frankfurt, Germany
Indrajit Ray	Colorado State University, USA
Carlos Rieder	ISec AG, Switzerland
Peter Ryan	University of Luxembourg, Luxembourg
Pierangela Samarati	Università degli Studi di Milano, Italy
Andrea Saracino	National Research Council of Italy, Italy
Damien Sauveron	University of Limoges, France
Nitesh Saxena	University of Alabama at Birmingham, USA
Abbas Shahim	VU University Amsterdam, The Netherlands
Ingrid Schaumüller-Bichl	FH Upper Austria, Austria
Einar Snekkenes	Gjovik University College, Norway
Adesina Sodiya	Federal University of Agric, Nigeria
Scott Stoller	Stony Brook University, USA
Bhavani Thuraisingham	The University of Texas at Dallas, USA
Paulo Verissimo	Universidade de Lisboa, Portugal
Rossouw Von Solms	NMMU, South Africa
Cong Wang	City University of Hong Kong, SAR China
Merrill Warkentin	Mississippi State University, USA
Edgar Weippl	SBA Research, Austria
Tatjana Welzer	University of Maribor, Slovenia
Steffen Wendzel	Hochschule Worms, Germany
Shengzhi Zhang	Florida Tech, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
André Zúquete	IEETA, Portugal

Additional Reviewers

Aysajan Abidin	Olivier Blazy
Mohsen Ahmadvand	Jonas Boehler
Muhamad Erza Aminanto	Dusan Bozilov
S. Abhishek Anand	Alexander Branitskiy
Afonso Arriaga	Jan-Willem Bullee
Arash Atashpendar	Enrico Cambiaso
Monir Azraoui	Michelle Cayford
Fabian Böhm	Andrea Ceccarelli
Sebastian Banescu	Andrey Chechulin
Iulia Bastys	Yueqiang Cheng
Gunjan Batra	Sabarathinam Chockalingam
Daniel Bernau	Rakyong Choi
Arne Bilzhause	Sutanay Choudhury
Anis Bkakria	Warren Connell

Anamaria Costache
Gianpiero Costantino
Kasper Damgaar
Vasily Desnitsky
Lena Doynikova
Kaoutar Elkhiyaoui
David Espes
Chris Everett
Andrey Fedorchenko
Gerardo Fernandez
Simon Foley
Simon Friedberger
Alexander Fromm
Benny Fuhry
Clemente Galdi
Mohamad Gharib
Laszlo Gonczy
Lenka Gondova
Sebastian Groll
Akos Grosz
Marko Hölbl
Florian Hahn
Lukas Hartmann
Majid Hatamian
Kirsi Helkala
Maximilian Hils
Erik Hjelmås
Petra Hochmannova
Matthias Hummer
Vincenzo Iovino
Katharina Issel
Leonardo Iwaya
Jaroslav Janáček
Jonas Lindstrøm Jensen
Olaf Markus Köhler
Johannes Köstler
Severin Kacianka
Christos Kalloniatis
Georgios Kambourakis
Maria Karyda
Marek Klein
Imre Kocsis
Mathias Kohler
Spyros Kokolakis
Andrea Kolberger
Marko Kompara
Tamas Kovacshazy
Katharina Krombholz
Michael Kunz
Stefan Laube
Ibrahim Lazrig
Laurens Lemaire
Fudong Li
Paolo Lollini
Sebastian Luhn
Clara Maathuis
Tobias Marktscheffel
Stefan Meier
Weizhi Meng
Francesco Mercaldo
Georg Merzdovnik
Zoltan Micskei
Tarik Moataz
Nurul Momen
Leonardo Montecchi
Subhojeet Mukherjee
Dieudonne Mulamba
Patrick Murmann
Ajaya Neupane
Ana Nieto
Tomasz Nowak
David Nuñez
Saahil Ognawala
Janos Olah
Maciej Olewiński
Melek Önen
Richard Ostertág
Jaemin Park
Juan D. Parra Rodriguez
Vinh Pham
Federico Pastorino
Cecilia Pasquini
Alexander Puchta
Tobias Pulls
Vincent Raes
Noëlle Rakotondravony
Evangelos Rekleitis
Jenni Reuben
Alfredo Rial
Christian Richthammer
Harmut Richthammer
Ruben Rios

Peter Roenne
Christian Roth
Johannes Saenger
Maliheh Shirvanian
Igor Saenko
Aleieldin Salem
Kiavash Satvat
Enrico Schiavone
Christopher Schmitz
Pascal Schoettle
Mariusz Sepczuk
Ankit Shah
Mina Sheikhalishahi
Prakash Shrestha
Dimitris E. Simos
Albert Sitek
Berit Skjernaa
Marjan Skrobot
Benjamin Smith
Martin Stanek
Michael Stausholm
Adam Szekeres
Masoud Tabatabaei
Tanay Talukdar
Benjamin Taubmann
Welderufael Tesfay
Alberto Trombetta
Anselme Tueno
Marcin Alan Tunia
Muhamed Turkanovic
Theodoros Tzouramanis
Ivan Vaccari
Cédric Van Rompay
Dimitrios Vasilopoulos
Sridhar Venkatesan
Fatbardh Veseli
Marcus Voelp
Jan Vossaert
Artemios Voyiatzis
Jun Wang
Michael Weber
Benjamin Weggenmann
Rea Yaich
Ahmed Seid Yesuf
Jonathan Yung
Tao Zhang
Tommaso Zoppi

Sponsor

Contents

Applied Cryptography and Voting Schemes

Software Security and Privacy

Privacy