Lecture Notes in Computer Science 11091

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

Sokratis K. Katsikas · Cristina Alcaraz (Eds.)

Security and Trust Management

14th International Workshop, STM 2018
Barcelona, Spain, September 6–7, 2018
Proceedings

Springer

Editors

Sokratis K. Katsikas
Open University of Cyprus
Latsia
Cyprus

and

Norwegian University of Science
and Technology
Gjøvik
Norway

Cristina Alcaraz
University of Malaga
Malaga
Spain

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-01140-6 ISBN 978-3-030-01141-3 (eBook)
https://doi.org/10.1007/978-3-030-01141-3

Library of Congress Control Number: 2018955425

LNCS Sublibrary: SL4 – Security and Cryptology

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

Preface

This volume contains the papers presented at the 14th International Workshop on Security and Trust Management (STM 2018). The workshop was co-located with the 23rd European Symposium on Research in Computer Security (ESORICS 2018) and was held in Barcelona, Spain, during September 6–7, 2018.

STM (Security and Trust Management) is a working group of ERCIM (European Research Consortium in Informatics and Mathematics). The STM workshop seeks submissions from academia, industry, and government that present novel research on all theoretical and practical aspects of security and trust in ICTs.

STM 2018 attracted 28 high-quality submissions, each of which was assigned to three referees for review; the review process resulted in eight full papers being accepted to be presented and included in the proceedings. These contributions cover topics related to cryptosystems and applied cryptography; modelling and risk assessment; and trust computing.

We would like to express our deepest thanks to all those who assisted us in organizing the event and putting together the program. We are very grateful to the ERCIM STM Steering Committee, and particularly its chair, Pierangela Samarati, for entrusting us with organizing the workshop; to Nicholas Kolokotronis, for taking care of publicity; to Joaquin Garcia-Alfaro (ESORICS 2018 Workshops Chair) and Miquel Soriano (ESORICS 2018 General Chair) for their support in organizing the workshop and taking care of the logistics. Special thanks go to the members of the Program Committee for their timely and rigorous reviews that helped us greatly in putting together a stimulating program. Last, but by no means least, we would like to thank all the authors who submitted their work to the workshop and contributed to an interesting set of proceedings.

August 2018

Sokratis K. Katsikas
Cristina Alcaraz

Organization

Sokratis Katsikas (Chair)	Open University of Cyprus, Cyprus and Norwegian University of Science and Technology, Norway
Cristina Alcaraz (Chair)	University of Malaga, Spain
Ken Barker	University of Calgary, Canada
David Chadwick	University of Kent, UK
Jorge Cuellar	Siemens AG, Corporate Technology, Germany
Sabrina De Capitani di Vimercati	University of Milan, Italy
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Carmen Fernández-Gago	University of Malaga, Spain
Sara Foresti	University of Milan, Italy
Joaquin Garcia-Alfaro	Telecom SudParis, France
Vasileios Gkioulos	Norwegian University of Science and Technology, Norway
Ehud Gudes	Ben-Gurion University, Israel
Nicholas Kolokotronis	University of the Peloponnese, Greece
Costas Lambrinoudakis	University of Piraeus, Greece
Giovanni Livraga	University of Milan, Italy
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Catherine Meadows	Naval Research Laboratory, USA
Chris Mitchell	Royal Holloway, University of London, UK
Charles Morisset	Newcastle University, UK
Pankaj Pandey	Norwegian University of Science and Technology, Norway
Günther Pernul	Universität Regensburg, Germany
Marinella Petrocchi	IIT-CNR, Italy
Benoit Poletti	Ministry of Economy/INCERT GIE, Luxembourg
Silvio Ranise	FBK-Irst, Italy
Pierangela Samarati	University of Milan, Italy
Ralf Sasse	ETH Zurich, Switzerland
Daniele Sgandurra	Royal Holloway, University of London, UK
Georgios Spathoulas	University of Thessaly, Greece
Fabian Van Den Broek	Open University in the Netherlands, The Netherlands

Contents

Cryptosystems and Applied Cryptography

Achieving Strong Security and Verifier-Local Revocation for Dynamic Group Signatures from Lattice Assumptions 3
Maharage Nisansala Sevwandi Perera and Takeshi Koshiba

Modular Verification of Sequential Composition for Private Channels in Maude-NPA 20
Fan Yang, Santiago Escobar, Catherine Meadows, and José Meseguer

A Spark Is Enough in a Straw World: A Study of Websites Password Management in the Wild 37
Simone Raponi and Roberto Di Pietro

A Fast and Scalable Fragmentation Algorithm for Data Protection Using Multi-storage over Independent Locations 54
Katarzyna Kapusta and Gerard Memmi

Modelling and Risk Assessment

Cyber Insurance Against Electronic Payment Service Outages: A Document Study of Terms and Conditions from Electronic Payment Service Providers and Insurance Companies. 73
Ulrik Franke

Semi-automatically Augmenting Attack Trees Using an Annotated Attack Tree Library 85
Ravi Jhawar, Karim Lounis, Sjouke Mauw, and Yunior Ramírez-Cruz

Trust Computing

Tux: Trust Update on Linux Booting. 105
Suhho Lee and Seehwan Yoo

Verifiable Outsourcing of Computations Using Garbled Onions 122
Tahsin C. M. Dönmez

Author Index 139