Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

Sara Foresti (Ed.)

Security and Trust Management

11th International Workshop, STM 2015
Vienna, Austria, September 21–22, 2015
Proceedings

Editor
Sara Foresti
Dipartimento di Informatica
Università degli Studi di Milano
Crema
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-24857-8 ISBN 978-3-319-24858-5 (eBook)
DOI 10.1007/978-3-319-24858-5

Library of Congress Control Number: 2015949450

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London
© Springer International Publishing Switzerland 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

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

Preface

These proceedings contain the papers selected for presentation at the 11th International Workshop on Security and Trust Management (STM 2015), held in Vienna, Austria, during September 21–22, 2015, in conjunction with the 20th European Symposium on Research in Computer Security (ESORICS 2015).

In response to the call for papers, 38 papers were submitted from 23 different countries. Each paper was reviewed by three members of the Program Committee, who considered its significance, novelty, technical quality, and practical impact in their evaluation. As in previous years, reviewing was double-blind, that is, the identities of reviewers were not revealed to the authors of the papers and identities of authors were not revealed to the reviewers. The Program Committee's work was carried out electronically, yielding intensive discussions over a period of one week. Of the submitted papers, the Program Committee accepted 15 full papers (resulting in an acceptance rate of 39.5%) and 4 short papers for presentation at the workshop. Besides the technical program including the papers collated in these proceedings, the workshop featured an invited talk by the winner of the ERCIM STM WG 2015 Award for the best PhD thesis on security and trust management.

The credit for the success of an event like STM 2015 belongs to a number of people, who devoted their time and energy to put together the workshop and who deserve acknowledgment. First of all, I wish to thank all the members of the Program Committee and all the external reviewers, for all their hard work in evaluating all the papers in a short time window, and for their active participation in the discussion and selection process. I would like to express my sincere gratitude to the ERCIM STM Steering Committee, and its chair, Pierangela Samarati, in particular, for their guidance and support in the organization of the workshop. Thanks to Giovanni Livraga, for taking care of publicity. I would also like to thank Javier Lopez (ESORICS Workshop Chair), Günther Pernul (ESORICS General Chair), and Yvonne Poul (ESORICS Local Organizer) for their support in the workshop organization and logistics.

Last but certainly not least, thanks to all the authors who submitted papers and to all the workshop's attendees. I hope you find the proceedings of STM 2015 interesting and of inspiration for your future research.

September 2015

Sara Foresti

Organization

Program Chair

Sara Foresti

Università degli Studi di Milano, Italy

Publicity Chair

Giovanni Livraga

Università degli Studi di Milano, Italy

STM Steering Committee

Theo Dimitrakos

British Telecom, UK

Javier Lopez

University of Málaga, Spain

Fabio Martinelli

National Research Council, Italy

Sjouke Mauw

University of Luxembourg, Luxembourg

Stig F. Mjølhusnes

NTNU, Norway

Pierangela Samarati (Chair)

Università degli Studi di Milano, Italy

Ulrich Ultes-Nitsche

University of Fribourg, Switzerland

Program Committee

Ken Barker

University of Calgary, Canada

David W. Chadwick

University of Kent, UK

Jorge Cuellar

Siemens AG, Germany

Sabrina De Capitani
di Vimercati

Università degli Studi di Milano, Italy

Theo Dimitrakos

British Telecom, UK

Josep Domingo-Ferrer

Universitat Rovira i Virgili, Spain

Carmen Fernández-Gago

University of Málaga, Spain

José-Luis Ferrer-Gomila

University of the Balearic Islands, Spain

Joaquin Garcia-Alfaro

Telecom SudParis, France

Ehud Gudes

Ben-Gurion University, Israel

Michael Huth

Imperial College London, UK

Christian D. Jensen

Technical University of Denmark, Denmark

Florian Kerschbaum

SAP, Germany

Costas Lambrinoudakis

University of Piraeus, Greece

Javier Lopez

University of Málaga, Spain

Evangelos Markatos

University of Crete, Greece

Stephen Marsh

University of Ontario, Institute of Technology, Canada

Fabio Martinelli

National Research Council, Italy

Sjouke Mauw

University of Luxembourg, Luxembourg

Catherine Meadows	Naval Research Laboratory, USA
Stig F. Mjøl̂snes	NTNU, Norway
Charles Morisset	Newcastle University, UK
Stefano Paraboschi	Università degli Studi di Bergamo, Italy
Siani Pearson	HP, UK
Günther Pernul	University of Regensburg, Germany
Marinella Petrocchi	National Research Council, Italy
Silvio Ranise	FBK, Italy
Carsten Rudolph	Huawei European Research Centre, Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Mohammad Torabi Dashti	ETH, Switzerland
Vicenç Torra	University of Skövde, Sweden
Claire Vishik	Intel Corporation, UK
Edgar Weippl	Vienna University of Technology, Austria
Nicola Zannone	TU/e, The Netherlands

External Reviewers

Mahdi Alizadeh	Martina Lindorfer
Alberto Blanco-Justicia	Stefan Meier
Joshua Daniel	Michael Netter
Malik Imran Daud	David Nuñez
Riccardo De Masellis	Pramod Pawar
Daniel Ricardo Dos Santos	Nikolaos Pitropakis
Alexandru Ionut Egner	Jordi Ribes-González
Ludwig Fuchs	Ali Sajjad
Jordi Herrera-Joancomarti	Johannes Sanger
Hugo Jonker	Andrea Saracino
Aljosha Judmayer	Giada Sciarretta
Ali El Kaafarani	Rolando Trujillo-Rasua
Yin Li	

Contents

Security Metrics and Classification

Digital Waste Sorting: A Goal-Based, Self-Learning Approach to Label Spam Email Campaigns	3
<i>Mina Sheikhalishahi, Andrea Saracino, Mohamed Mejri, Nadia Tawbi, and Fabio Martinelli</i>	
Integrating Privacy and Safety Criteria into Planning Tasks	20
<i>Anna Lavygina, Alessandra Russo, and Naranker Dulay</i>	
Security Metrics, Secure Elements, and Operational Measurement Trust in Cloud Environments	37
<i>Teemu Kanstrén and Antti Evesti</i>	

Data Protection

A Declarative Framework for Specifying and Enforcing Purpose-Aware Policies	55
<i>Riccardo De Masellis, Chiara Ghidini, and Silvio Ranise</i>	
How to Trust the Re-use of Data	72
<i>Erisa Karafil, Hanne Riis Nielson, and Flemming Nielson</i>	
Towards Balancing Privacy and Efficiency: A Principal-Agent Model of Data-Centric Business	89
<i>Christian Zimmermann and Claus-Georg Nolte</i>	

Intrusion Detection and Software Vulnerabilities

The AC-Index: Fast Online Detection of Correlated Alerts	107
<i>Andrea Pugliese, Antonino Rullo, and Antonio Piccolo</i>	
Intrusion Detection System for Applications Using Linux Containers.	123
<i>Amr S. Abed, Charles Clancy, and David S. Levy</i>	
SUDUTA: Script UAF Detection Using Taint Analysis	136
<i>John Galea and Mark Vella</i>	

Cryptographic Protocols

Two-Factor Authentication for the Bitcoin Protocol.	155
<i>Christopher Mann and Daniel Loebenberger</i>	

Private Proximity Testing on Steroids: An NTRU-Based Protocol	172
<i>Constantinos Patsakis, Panayiotis Kotzanikolaou, and Mélanie Bourroche</i>	

Selecting a New Key Derivation Function for Disk Encryption	185
<i>Milan Brož and Vashek Matyáš</i>	

Controlling Data Release

It's My Privilege: Controlling Downgrading in DC-Labels	203
<i>Lucas Waye, Pablo Buiras, Dan King, Stephen Chong, and Alejandro Russo</i>	

Obligations in PTaCL	220
<i>Jason Crampton and Conrad Williams</i>	

Content and Key Management to Trace Traitors in Broadcasting Services . . .	236
<i>Kazuto Ogawa, Goichiro Hanaoka, and Hideki Imai</i>	

Security Analysis, Risk Management, and Usability

In Cyber-Space No One Can Hear You S-CREAM: A Root Cause Analysis for Socio-Technical Security	255
<i>Ana Ferreira, Jean-Louis Huynen, Vincent Koenig, and Gabriele Lenzini</i>	

A Socio-Technical Investigation into Smartphone Security	265
<i>Melanie Volkamer, Karen Renaud, Oksana Kulyk, and Sinem Emeröz</i>	

A Game Theoretic Framework for Modeling Adversarial Cyber Security Game Among Attackers, Defenders, and Users	274
<i>Tatyana Ryutov, Michael Orosz, James Blythe, and Detlof von Winterfeldt</i>	

Design, Demonstration, and Evaluation of an Information Security Contract and Trading Mechanism to Hedge Information Security Risks	283
<i>Pankaj Pandey and Steven De Haes</i>	

Author Index	293
-------------------------------	-----