

*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, Zurich, 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>

Giovanni Livraga · Chris Mitchell (Eds.)

# Security and Trust Management

13th International Workshop, STM 2017  
Oslo, Norway, September 14–15, 2017  
Proceedings

*Editors*

Giovanni Livraga   
Università degli Studi di Milano  
Crema  
Italy

Chris Mitchell  
University of London  
Egham  
UK

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-68062-0              ISBN 978-3-319-68063-7 (eBook)  
DOI 10.1007/978-3-319-68063-7

Library of Congress Control Number: 2017953412

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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 13th International Workshop on Security and Trust Management (STM 2017), held in Oslo, Norway, on September 14–15, 2017, in conjunction with the 22th European Symposium On Research In Computer Security (ESORICS 2017).

In response to the call for papers, 33 papers were submitted, and all submissions were evaluated on the basis of their significance, novelty, and technical quality. The Program Committee, comprising 30 members, performed an excellent task and with the help of additional reviewers all submissions went through a careful anonymous review process (three or more reviews per submission). 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 ten full papers and six 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 2017 Award for the best PhD thesis on security and trust management.

The credit for the success of STM 2017 belongs to a number of people, who devoted their time and energy to put together the workshop and deserve acknowledgment. We would like to thank all the members of the Program Committee and all the external reviewers, for their hard work in evaluating all the papers in a short time window, and for their active participation in the discussion and selection process. We are very grateful to everyone who gave assistance and ensured a smooth organization process: the ERCIM STM Steering Committee, and in particular its chair, Pierangela Samarati, for their guidance and support in the organization of the workshop; Angelo Genovese, for taking care of publicity; Sokratis Katsikas (ESORICS Workshop Chair), Einar Snekkenes (ESORICS General Chair), and Laura Georg (ESORICS Organization Chair), 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 attendees. We hope you find the proceedings of STM 2017 interesting and an inspiration for your future research.

August 2017

Giovanni Livraga  
Chris Mitchell

# Organization

## Program Chairs

Giovanni Livraga                      Università degli Studi di Milano, Italy  
Chris Mitchell                          Royal Holloway, University of London, UK

## Publicity Chair

Angelo Genovese                      Università degli Studi di Milano, Italy

## STM Steering Committee

Theo Dimitrakos                      University of Kent, UK  
Javier Lopez                          University of Malaga, Spain  
Fabio Martinelli                      CNR, Italy  
Sjouke Mauw                        Université of Luxembourg, Luxembourg  
Stig F. Mjøl̄snes                      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  
Colin Boyd                          NTNU, Norway  
David Chadwick                      University of Kent, UK  
Liqun Chen                        University of Surrey, UK  
Jorge Cuéllar                      Siemens AG, Germany  
Sabrina De Capitani  
di Vimercati                        Università degli Studi di Milano, Italy  
Josep Domingo-Ferrer              Universitat Rovira i Virgili, Spain  
Sara Foresti                        Università degli Studi di Milano, Italy  
Joaquin Garcia-Alfaro              Telecom SudParis, France  
Ehud Gudes                        Ben-Gurion University, Israel  
Michael Huth                        Imperial College, UK  
Costas Lambrinouidakis            University of Piraeus, Greece  
Javier Lopez                        University of Malaga, Spain  
Fabio Martinelli                      CNR, Italy  
Sjouke Mauw                        University of Luxembourg, Luxembourg  
Catherine Meadows                NRL, USA  
Stig F. Mjøl̄snes                      NTNU, Norway  
Charles Morisset                    Newcastle University, UK  
Siani Pearson                        HP, UK

Günther Pernul	University of Regensburg, Germany
Marinella Petrocchi	CNR, Italy
Benoit Poletti	INCERT GIE, Luxembourg
Silvio Ranise	FBK, Italy
Ralf Sasse	ETH Zurich, Switzerland
Daniele Sgandurra	Royal Holloway, University of London, UK
Vicenç Torra	University of Skövde, Sweden
Fabian Van Den Broek	Radboud University of Nijmegen, The Netherlands
Vijay Varadharajan	University of Newcastle, Australia
Damien Vergnaud	ENS, France
Cong Wang	City University of Hong Kong, Hong Kong, SAR China

### **Additional Reviewers**

Alexey Rabin	Andrea Saracino
Michael Hitchens	Luis Del Vasto
Sietse Ringers	Udaya Tupakula
Michael Kunz	Sergio Martinez
Florian Menges	Imad Mahaini
Patrick Ah-Fat	Sean Simpson
Fabian Böhm	Andrea Callia D’Iddio
Francesco Mercaldo	Carmen Fernandez
Rolando Trujillo	Brinda Hampiholi

# Contents

## Cryptosystems and Applied Cryptography

Key Management for Versatile Pay-TV Services . . . . .	3
<i>Kazuto Ogawa, Sakurako Tamura, and Goichiro Hanaoka</i>	
Dynamic Similarity Search over Encrypted Data with Low Leakage . . . . .	19
<i>Daniel Homann, Christian Göge, and Lena Wiese</i>	
Enhanced Modelling of Authenticated Key Exchange Security . . . . .	36
<i>Papa B. Seye and Augustin P. Sarr</i>	

## Software Security and Risk Management

Authentic Execution of Distributed Event-Driven Applications with a Small TCB . . . . .	55
<i>Job Noorman, Jan Tobias Mühlberg, and Frank Piessens</i>	
Exploring Botnet Evolution via Multidimensional Models and Visualisation . . .	72
<i>William Dash and Matthew J. Craven</i>	
Facing Uncertainty in Cyber Insurance Policies. . . . .	89
<i>Per Håkon Meland, Inger Anne Tøndel, Marie Moe, and Fredrik Seehusen</i>	

## Authorization

How Much is Risk Increased by Sharing Credential in Group? . . . . .	103
<i>Hiroaki Kikuchi, Niihara Koichi, and Michihiro Yamada</i>	
Smart Parental Advisory: A Usage Control and Deep Learning-Based Framework for Dynamic Parental Control on Smart TV. . . . .	118
<i>Giacomo Giorgi, Antonio La Marra, Fabio Martinelli, Paolo Mori, and Andrea Saracino</i>	
A Consistent Definition of Authorization . . . . .	134
<i>Audun Jøsang</i>	

## Security Vulnerabilities and Protocols

Formal Analysis of V2X Revocation Protocols . . . . .	147
<i>Jorden Whitefield, Liqun Chen, Frank Kargl, Andrew Paverd, Steve Schneider, Helen Treharne, and Stephan Wesemeyer</i>	



Refinement-Aware Generation of Attack Trees . . . . .	164
<i>Olga Gadyatskaya, Ravi Jhawar, Sjouke Mauw, Rolando Trujillo-Rasua, and Tim A.C. Willemse</i>	
Exploit Prevention, Quo Vadis? . . . . .	180
<i>László Erdődi and Audun Jøsang</i>	
<b>Secure Systems</b>	
Estimating Software Obfuscation Potency with Artificial Neural Networks . . .	193
<i>Daniele Canavese, Leonardo Regano, Cataldo Basile, and Alessio Viticchié</i>	
EigenTrust for Hierarchically Structured Chord. . . . .	203
<i>Kalonji Kalala, Tao Feng, and Iluju Kiringa</i>	
Cover Traffic: A Trade of Anonymity and Efficiency . . . . .	213
<i>Tim Grube, Markus Thummerer, Jörg Daubert, and Max Mühlhäuser</i>	
Quantitative Analysis of DoS Attacks and Client Puzzles in IoT Systems. . . .	224
<i>Luca Arnaboldi and Charles Morisset</i>	
<b>Author Index</b> . . . . .	235