

## Founding Editors

Gerhard Goos

*Karlsruhe Institute of Technology, Karlsruhe, Germany*

Juris Hartmanis

*Cornell University, Ithaca, NY, USA*

## Editorial Board Members

Elisa Bertino

*Purdue University, West Lafayette, IN, USA*

Wen Gao

*Peking University, Beijing, China*

Bernhard Steffen 

*TU Dortmund University, Dortmund, Germany*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung 

*Columbia University, New York, NY, USA*


More information about this subseries at <https://link.springer.com/bookseries/7410>


Rodrigo Roman · Jianying Zhou (Eds.)

# Security and Trust Management

17th International Workshop, STM 2021  
Darmstadt, Germany, October 8, 2021  
Proceedings

*Editors*

Rodrigo Roman   
University of Málaga  
Málaga, Spain

Jianying Zhou   
Singapore University of Technology  
and Design  
Singapore, Singapore

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-91858-3              ISBN 978-3-030-91859-0 (eBook)  
<https://doi.org/10.1007/978-3-030-91859-0>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021

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, expressed 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.

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

# Preface

These proceedings contain the papers selected for presentation at the 17th International Workshop on Security and Trust Management (STM 2021) held as an online event on October 8, 2021, in conjunction with the 26th European Symposium on Research in Computer Security (ESORICS 2021). As in the previous year, due to the ongoing COVID-19 situation ESORICS 2021 and the associated workshops – including STM 2021 – ran as an all-digital conference experience.

This year we initiated two rounds of the call for papers, the first in July 2021 and the second in August 2021, which in total attracted 26 high-quality submissions. Each submission was assigned to three referees for review and, as in previous years, reviewing was double-blind. The review process resulted in ten full papers – an acceptance rate of 38% – being accepted for presentation and included in the proceedings. These contributions cover topics related to applied cryptography; privacy; formal methods for security and trust; and systems security.

As in previous editions, the program of the STM 2021 workshop also featured an invited talk by the recipient of the 2021 ERCIM STM Best PhD Award. The laureate of this year was Jo Van Bulck for his thesis “Microarchitectural Side-Channel Attacks for Privileged Software Adversaries,” written at the Katholieke Universiteit Leuven (KU Leuven), Belgium.

This year we also introduced the Best Paper Award. The selection was based on review comments from Program Committee (PC) members as well as the paper’s overall quality. The award went to Korbinian Spielvogel, Henrich C. Pöhls, and Joachim Posegga for their paper “TLS beyond the broker: Enforcing fine-grained security and trust in publish/subscribe environments for IoT”.

We would like to thank all the people that helped us in the organization of this event. In no particular order, thanks to Pierangela Samarati, chair of the Security and Trust Management Working Group, for her support and advice during the organization of the workshop; to Weizhi Meng, publicity chair, to help us bring this workshop to the eyes of all contributors; to all the members of the Program Committee and external reviewers, who endured two rounds of submissions and provided the authors with excellent feedback; to all the authors who submitted papers; and to all the attendees for contributing to the workshop discussions.

We also want to thank you, the reader, for picking up this volume. We hope that the contents of these proceedings will inspire you and help you in your future research.

October 2021

Rodrigo Roman  
Jianying Zhou

# Organization

## Program Chairs

Rodrigo Roman  
Jianying Zhou

University of Málaga, Spain  
SUTD, Singapore

## Publicity Chair

Weizhi Meng

Technical University of Denmark, Denmark

## Program Committee

Cristina Alcaraz  
Pasquale Annicchino  
Joonsang Baek  
Mauro Conti  
Said Daoudagh  
Sabrina De Capitani di  
Vimercati  
Roberto Di Pietro  
Carmen Fernandez Gago  
Olga Gadyatskaya  
Dieter Gollmann  
Jinguang Han  
Marko Hölbl  
Chenglu Jin  
Panayiotis Kotzanikolaou  
Giovanni Livraga  
Bo Luo  
Xiapu Luo  
Fabio Martinelli  
Daisuke Mashima  
Sjouke Mauw  
Keith Mayes  
Weizhi Meng  
Chuahry Mujeeb Ahmed  
Surya Nepal  
Liliana Pasquale  
Joachim Posegga  
Davy Preuveneers  
Pierangela Samarati  
Qingni Shen

University of Malaga, Spain  
Archimede Solutions, Switzerland  
University of Wollongong, Australia  
University of Padua, Italy  
ISTI-CNR, Italy  
Università degli Studi di Milano, Italy  
Hamad Bin Khalifa University, Qatar  
University of Malaga, Spain  
Leiden University, The Netherlands  
TUHH, Germany  
Queen's University Belfast, UK  
University of Maribor, Slovenia  
Centrum Wiskunde & Informatica, The Netherlands  
University of Piraeus, Greece  
Università degli Studi di Milano, Italy  
University of Kansas, USA  
The Hong Kong Polytechnic University, Hong Kong  
IIT-CNR, Italy  
ADSC, Singapore  
University of Luxembourg, Luxembourg  
Royal Holloway, University of London, UK  
Technical University of Denmark, Denmark  
University of Strathclyde, UK  
Data 61, Australia  
University College Dublin, Ireland  
University of Passau, Germany  
KU Leuven, Belgium  
Università degli Studi di Milano, Italy  
Peking University, China

Marco Squarcina	TU Wien, Austria
Chunhua Su	University of Aizu, Japan
Yangguang Tian	Osaka University, Japan
Hiroshi Tsunoda	Tohoku Institute of Technology, Japan
Zheng Yang	SUTD, Singapore
Chia-Mu Yu	National Chiao Tung University, Taiwan

## **External Reviewers**

Sergiu Bursuc  
Maryam Ehsanpour  
Alzubair Hassan  
Gulshan Kumar  
Eleonora Losiouk  
Elizabeth Quaglia  
Korbinian Spielvogel  
Utku Tefek  
Pengfei Wu

# Contents

## Applied Cryptography

An Aggregate Signature with Pre-communication in the Plain Public Key Model. . . . .	3
<i>Masayuki Fukumitsu and Shingo Hasegawa</i>	
The Adversary Capabilities in Practical Byzantine Fault Tolerance . . . . .	20
<i>Yongge Wang</i>	

## Privacy

Where to Meet a Driver Privately: Recommending Pick-Up Locations for Ride-Hailing Services. . . . .	43
<i>Yifei Chen, Meng Li, Shuli Zheng, Chhagan Lal, and Mauro Conti</i>	
Efficient Permutation Protocol for MPC in the Head . . . . .	62
<i>Peeter Laud</i>	
Efficient Scalable Multi-party Private Set Intersection Using Oblivious PRF . . . . .	81
<i>Alireza Kavousi, Javad Mohajeri, and Mahmoud Salmasizadeh</i>	

## Formal Methods for Security and Trust

Secure Implementation of a Quantum-Future GAKE Protocol. . . . .	103
<i>Robert Abela, Christian Colombo, Peter Malo, Peter Sýs, Tomáš Fabšič, Ondrej Gallo, Viliam Hromada, and Mark Vella</i>	
Deciding a Fragment of $(\alpha, \beta)$ -Privacy. . . . .	122
<i>Laouen Fernet and Sebastian Mödersheim</i>	

## Systems Security

TLS Beyond the Broker: Enforcing Fine-Grained Security and Trust in Publish/Subscribe Environments for IoT . . . . .	145
<i>Korbinian Spieltogel, Henrich C. Pöhls, and Joachim Posegga</i>	
Root-of-Trust Abstractions for Symbolic Analysis: Application to Attestation Protocols . . . . .	163
<i>Georgios Fotiadis, José Moreira, Thanassis Giannetsos, Liqun Chen, Peter B. Rønne, Mark D. Ryan, and Peter Y. A. Ryan</i>	



**Towards Decentralized and Provably Secure Cross-Domain Solutions . . . . .**    185  
    *Joud Khoury, Zachary Ratliff, and Michael Atighetchi*

**Author Index . . . . .**    205