

*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>

Jan Camenisch · Doğan Kesdoğan (Eds.)

# Open Problems in Network Security

IFIP WG 11.4 International Workshop, iNetSec 2015  
Zurich, Switzerland, October 29, 2015  
Revised Selected Papers

*Editors*

Jan Camenisch  
IBM Research Zurich  
Rueschlikon  
Switzerland

Doğan Kesdoğan  
University of Regensburg  
Regensburg  
Germany

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-39027-7              ISBN 978-3-319-39028-4 (eBook)  
DOI 10.1007/978-3-319-39028-4

Library of Congress Control Number: 2016939100

LNCS Sublibrary: SL4 – Security and Cryptology

© IFIP International Federation for Information Processing 2016

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

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG Switzerland

# Preface

The international workshop iNetSec—Open Problems in Network Security—is the main workshop of the IFIP working group WG 11.4. Its objective is to present and discuss open problems and new research directions on all aspects related to network security.

Before 2009, iNetSec followed the traditional format where research papers were submitted, peer-reviewed, and then presented at the workshop. In 2009, this was changed into a format in which the discussion of open research problems and directions at the workshop becomes an integral part of the paper publication process. To enable this open workshop style yet remain focused on particular topics, we called for two-page abstracts in which the authors were asked to outline open research problems and new directions in network security. These abstracts were reviewed by the entire Program Committee, who ranked each of them according to whether the problem presented was relevant and suited for a discussion. At the workshop, we reserved almost as much time for each topic presentation as for its discussion, which was half an hour. After the workshop, the authors were asked to submit full papers based on their abstracts and the discussions at the workshop. These papers were reviewed and those with the highest ranks were selected for these proceedings. May they serve as a source of inspiration for new research!

We thank IBM Research – Zurich for hosting the workshop, the Program Committee for reviewing papers, as well as the authors of all submissions that enabled iNetSec 2015 to be take place. And last but not least, we are grateful to all participants for their contribution to the lively discussions.

April 2016

Jan Camenisch  
Doğan Kesdoğan  
Dang Vinh Pham

# Organization

## Executive Committee

### Program Chairs

Jan Camenisch IBM Research – Zurich, Switzerland  
Doğan Kesdoğan University of Regensburg, Germany

### Organizing Chairs

Jan Camenisch IBM Research – Zurich, Switzerland  
Dang Vinh Pham University of Regensburg, Germany

### Program Committee

Jan Camenisch IBM Research – Zurich, Switzerland  
Hannes Federrath University of Hamburg, Germany  
Felix Freiling Friedrich Alexander University FAU, Germany  
Doğan Kesdoğan University of Regensburg, Germany  
Albert Levi Sabanci University, Turkey  
Javier Lopez University of Malaga, Spain  
Adrian Perrig ETH Zurich, Switzerland  
Dang Vinh Pham University of Regensburg, Germany  
Siraj A. Shaikh Coventry University, UK

# Contents

## Network Security

Forwarding Accountability: A Challenging Necessity of the Future Data Plane . . . . .	3
<i>Christos Pappas, Raphael M. Reischuk, and Adrian Perrig</i>	
A Metric for Adaptive Routing on Trustworthy Paths . . . . .	11
<i>Christoph Hofmann, Elke Franz, and Silvia Santini</i>	

## Intrusion Detection

Early Warning Systems for Cyber Defence. . . . .	29
<i>Harsha Kalutarage, Siraj Shaikh, Bu-Sung Lee, Chonho Lee, and Yeo Chai Kiat</i>	
Catching Inside Attackers: Balancing Forensic Detectability and Privacy of Employees . . . . .	43
<i>Ephraim Zimmer, Jens Lindemann, Dominik Herrmann, and Hannes Federrath</i>	
Intrusion Detection in the Smart Grid Based on an Analogue Technique . . . .	56
<i>Hartmut Richthammer and Sebastian Reif</i>	

## Anonymous Communication

On Building Onion Routing into Future Internet Architectures . . . . .	71
<i>Daniele E. Asoni, Chen Chen, David Barrera, and Adrian Perrig</i>	
Anonymity Online for Everyone: What Is Missing for Zero-Effort Privacy on the Internet?. . . . .	82
<i>Dominik Herrmann, Jens Lindemann, Ephraim Zimmer, and Hannes Federrath</i>	

## Cryptography

Reviving the Idea of Incremental Cryptography for the Zettabyte Era Use Case: Incremental Hash Functions Based on SHA-3 . . . . .	97
<i>Hristina Mihajloska, Danilo Gligoroski, and Simona Samardjiska</i>	
The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication . . . . .	112
<i>Marko Vukolić</i>	

<b>Author Index</b> . . . . .	127
-------------------------------	-----